SUPREME COURT OF INDIA

CIVIL WRIT PETITION 829 / 2013

IN THE MATTER OF:

S.G. VOMBATKERE & ANR. ...PETITIONERS

Versus

UNION OF INDIA & ORS. ...RESPONDENTS

COMPILATION

VOLUME IV – A

FOREIGN CASE - LAWS

(Pages 1 - 258)

(See Inside for Complete Index)

Submitted on behalf of the Petitioners

VOLUME IV

FOREIGN CASE LAWS

988 F.2d 1344, 61 USLW 2585, Unempl.Ins.Rep. (CCH) P 17193A
(Cite as: 988 F.2d 1344)

▷

United States Court of Appeals,
Fourth Circuit.
Marc Alan GREIDINGER, Plaintiff–Appellant,
v.
Bobby Ray DAVIS, Chairman; John H. Russ, Jr., Vice–Chairman; Michael G. Brown, Defendants–Appellees,
and
Ray H. Davis, General Registrar, Defendant.
Computer Professionals for Social Responsibility, Amicus Curiae.

No. 92–1571.
Argued Oct. 2, 1992.
Decided March 22, 1993.

Action was brought challenging requirement that voter supply social security number when registering to vote, which would then be made available to those purchasing voter registration lists. The United States District Court for the Eastern District of Virginia, James R. Spencer, J., 782 F.Supp. 1106, denied the relief sought, and applicant appealed. The Court of Appeals, Hamilton, Circuit Judge, held that: (1) state's practice of requiring social security numbers on voter registration applications and then making voter registration lists with the social security numbers available to the public infringed on the right to vote; and (2) the burden was not narrowly tailored to meet the state's interest in preventing voter fraud.

Reversed and remanded.

West Headnotes

[1] Election Law 142T ⚿62

142T Election Law
142TIII Voters
142TIII(B) Qualifications
142Tk61 Constitutional and Statutory Provisions
142Tk62 k. In general; power to regulate qualifications. Most Cited Cases
(Formerly 144k18 Elections)
Despite the fundamental nature of the right to vote, states may nevertheless impose certain qualifications on and regulate access to the franchise.

[2] Election Law 142T ⚿62

142T Election Law
142TIII Voters
142TIII(B) Qualifications
142Tk61 Constitutional and Statutory Provisions
142Tk62 k. In general; power to regulate qualifications. Most Cited Cases
(Formerly 144k18 Elections)
If substantial burden on right to vote exists, restrictions on the right must serve compelling state interest and be narrowly tailored to serve the state interest.

[3] Election Law 142T ⚿118

142T Election Law
142TIII Voters
142TIII(C) Registration
142Tk117 Proceedings for Registration
142Tk118 k. In general. Most Cited Cases
(Formerly 144k19 Elections)

Election Law 142T ⚿127

142T Election Law
142TIII Voters
142TIII(C) Registration
142Tk127 k. Filing or posting lists. Most Cited Cases
(Formerly 144k19 Elections)
State voter registration scheme which required voter to supply social security number and then allowed voter registration list which contained the voters' social security numbers to be purchased by others imposed a substantial burden on the right to

vote, but only to the extent that it permitted public disclosure of social security number. Va.Code 1950, §§ 24.1–23(8), 24.1–56.

[4] Election Law 142T ⚿127

142T Election Law
142TIII Voters
142TIII(C) Registration
142Tk127 k. Filing or posting lists. Most Cited Cases
(Formerly 144k19 Elections)

Disclosure as part of voter registration list of voters' social security numbers which they were required to supply when registering to vote was not narrowly tailored to fulfill State's interest in using social security numbers to prevent voter fraud and the State's interest thus could not justify the infringement on the right to vote. Va.Code 1950, §§ 24.1–23(8), 24.1–56.

*1345 Paul Reinherz Wolfson, Public Citizen Litigation Group, Washington, DC, for plaintiff-appellant.

Roger Conant Wiley, Jr., Sr. Asst. Atty. Gen., Office of the Attorney General, Richmond, VA, argued (Mary Sue Terry, Atty. Gen. of Va., K. Marshall Cook, Deputy Atty. Gen., Martha B. Brissette, Asst. Atty. Gen., Office of the Attorney General, on the brief), for defendants-appellees.

Marc Rotenberg, David L. Sobel, Computer Professionals for Social Responsibility, Washington, DC, for amicus curiae.

Before RUSSELL and HAMILTON, Circuit Judges, and TRAXLER, United States District Judge for the District of South Carolina, sitting by designation.

OPINION

HAMILTON, Circuit Judge:

As a consequence of registering to vote in the Commonwealth of Virginia (Virginia), a registered voter's Social Security number (SSN) is subject to public inspection in the Office of the General Registrar and provided upon request to, among other entities, political parties as part of voter registration lists. Applying strict scrutiny, the district court held that these provisions of Virginia's voter registration scheme do not violate appellant's fundamental right to vote. *Greidinger v. Davis*, 782 F.Supp. 1106 (E.D.Va.1992). We now reverse.

I

The Constitution of Virginia requires all citizens otherwise qualified to vote and possessing a SSN (registering after July 1, 1971) to provide their SSN on their Virginia Voter Registration Application (Application) in order to become registered to vote. Va. Const. art. II, § 2. If an individual otherwise qualified to vote does not possess a SSN, a "dummy" number will be provided. The scheme also provides that any registered voter may inspect the voter registration books in the Office of the General Registrar. In practice, these books contain the registration application of a registered voter. Va.Code Ann. § 24.1–56 (§ 24.1–56).

The scheme further provides that Statewide Voter Registration lists containing the SSNs of voters can be obtained by: (a) candidates for election to further their candidacy, (b) political party committees for political purposes only, (c) incumbent office holders to report to their constituents, and (d) nonprofit organizations which promote voter participation and registration for that purpose only. Va.Code Ann. § 24.1–23(8) (§ 24.1–23(8)). FN1

FN1. Those parties obtaining the computerized voting lists pursuant to § 24.1–23(8) must sign an oath averring to limit the use of the computerized voter lists to the specific purposes enumerated in the statute. *See infra* note 6. The record also reflects that the current cost of a statewide voter registration list is $5,700.

On July 24, 1991, appellant, Marc Alan

Greidinger, filled out an Application, but refused to disclose his SSN. Because of this omission, Greidinger received a Denial of Application for Virginia Voter Registration from the General Registrar of Stafford County. Consequently, the Virginia State *1346 Board of Elections (the Board) prevented Greidinger from voting in the November 5, 1991, general election. The Application completed by Greidinger did not state whether disclosure of his SSN was mandatory or voluntary, by what statutory or other authority the SSN was requested, what uses would be made of the SSN, or that the SSN might be disseminated to registered voters or political parties.

On August 22, 1992, Greidinger instituted this action *pro se* against Robert H. Davis, Greidinger's local registrar,[FN2] Bobby W. Davis, John H. Russ, Jr., and Michael G. Brown, who collectively comprise the Board.[FN3] Greidinger sought preliminary and permanent injunctive relief, declaratory relief, writs of mandamus and prohibition, costs and attorney's fees. Greidinger alleged that to the extent Virginia authorizes the collection and publication of SSNs for voter registration, it unconstitutionally burdens his right to vote. Greidinger also alleged that Virginia's Voter Registration Application violates § 7(b) of the Privacy Act of 1974, Pub.L. No. 93–579, § 7, 88 Stat. 1896, 1909 (1974), *reprinted in* 5 U.S.C. § 552a note (1982) (Privacy Act of 1974 or Privacy Act), because it did not: (a) specify whether the disclosure of the SSN was mandatory or voluntary, (b) inform him by what statutory or other authority his SSN was solicited, and (c) specify what uses would be made of his SSN.

> FN2. By agreement of the parties, Robert H. Davis was dismissed as a defendant.
>
> FN3. The State Board of Elections oversees local registrars, publishes a handbook of procedures, maintains the statewide computerized voter registration system, and prescribes voter registration cards and forms. Local registrars supervise voter registration, assist local electoral boards in conducting elections and maintain records required by law. Va.Code Ann. § 24.1–19 and § 24.1–46.

The parties filed cross-motions for summary judgment based upon stipulated facts. In pertinent part, the stipulation provided:

> (1) Marc Alan Greidinger ("Greidinger") is a resident of Stafford County, Virginia, and is fully qualified to register to vote under the laws of the Commonwealth of Virginia.
>
> ....
>
> (6) The Virginia Voter Registration Application[ ] completed by Greidinger ... did not specify whether disclosure of the social security account number is mandatory or voluntary, by what statutory or other authority the number was requested, or what uses would be made of the number[ ], or the specific consequences of not providing the number[ ], or the possible dissemination of the number[ ], nor [was] Greidinger notified of these facts by the Defendants before [he] applied to register to vote ... Greidinger [did not] ask[ ] for any of this information at the time [he] applied to register to vote.
>
> ....
>
> (15) The Commonwealth of Virginia has an interest in obtaining and using social security numbers of registered voters to provide a means of positive identification and prevent voter fraud, and in making voter registration information available to the public. However, no state interest is served by disclosing the social security numbers of voters to private individuals who request voter information from local registrars in the Commonwealth of Virginia.
>
> (16) The State Board of Elections has no prescribed procedure to prevent private individuals who request voter information at the offices of a local registrar from using voters' social security numbers for purposes unrelated to the electoral

process. The State Board of Elections' position is that no law requires it to have such a procedure, and it is further the State Board of Elections' position that no such procedure can effectively be devised.

(17) The State Board of Elections discloses voter lists containing voters' social security numbers to political parties and candidates in order to enable the two major political parties to keep track of voters when they move from place to place.

*1347 (18) The Virginia State Board of Elections prepares lists of registered voters and supplies these lists to local registrars prior to each general election. The statewide voter registration database is maintained and updated on a continuing basis by local registrars.

(19) Social security numbers of applicants for voter registration are not routinely verified. The State Board of Elections believes that such requirement would necessitate approval by the U.S. Department of Justice under the Federal Voting Rights Act. However, local registrars ask for verification of social security numbers when, it appears to be the same as the social security number of a previously registered voter.

(20) The Virginia State Board of Elections does not provide information regarding registered voters to any Virginia Governmental Agency other than those to which information is required to be disclosed pursuant to the Virginia Code.

....

(22) The Virginia State Board of Elections is unaware of any situations in which political parties or candidates for office, upon examination of Voter Registration Lists, have prevented voter fraud through the use of social security numbers of Registered Voters. However, the Virginia State Board of Elections frequently uses the social security number to identify duplicate registration, thereby helping to prevent voter fraud.

Joint Appendix (J.A.) at 36–40.

On January 17, 1992, the district court held that the Board did not comply with § 7(b) of the Privacy Act. *Greidinger v. Davis*, 782 F.Supp. at 1108–09. As a result, the district court ordered the Board to submit a schedule for prospective compliance with § 7(b) of the Privacy Act and to submit a summary of the measures to be taken to effectuate compliance with the notice requirements of § 7(b). The district court went on to reject Greidinger's constitutional challenge to Virginia's voter registration scheme. *Id.* at 1109–10. Applying strict scrutiny, the district court reasoned that Virginia's voter registration scheme was necessary to promote the compelling state interest of conducting fair and honest elections.[FN4] The district court observed that numerous state interests were advanced by the Virginia voter registration scheme, namely: the scheme eliminated voter duplication and possible fraud; allowed Virginia to keep track of voters who move to different locales; and assisted Virginia in eliminating disqualified voters from voter lists. *Id.* at 1110. Finally, the district court denied Greidinger's request for attorneys' fees, reasoning that the Privacy Act limits any award of fees and costs to willful or intentional conduct. *Id.* at 1110–11.

> FN4. In reaching this conclusion, the district court characterized the burden on Greidinger's fundamental right to vote as "minimal." *Greidinger v. Davis*, 782 F.Supp. at 1110.

Prior to the district court's decision, the Board began to draft a proposed Privacy Act notice to be used with new registration forms. The day after the district court's decision, the Board submitted a proposed notice to comply with the dictates of the Privacy Act. This notice was to be posted at all voter registration sites. The new notice informed registrants that the SSN was required under Va. Const. art. II, § 2. The notice also stated that the voter registration card containing the voter's SSN would become part of the permanent voting records and

would be open to inspection by any Virginia voter. Finally, the notice stated that computerized listings containing the information on the voter registration would be furnished upon request to elected officeholders, candidates for office, political parties, courts, and nonprofit organizations promoting voter participation and registration, for use on a restricted basis. *See infra* note 6.

On January 27, 1992, Greidinger filed a motion to alter or amend the district court's judgment. On February 12, 1992, the district court rejected Greidinger's request, finding no errors or mistakes which required correction. On March 17, 1992, Greidinger filed a motion for entry of final *1348 judgment on his constitutional claim, followed by a motion for reconsideration. On May 1, 1992, the district court entered a final judgment and order, finding that the proposed Privacy Act notice complied with the mandates of the Privacy Act and denying Greidinger's motion for reconsideration. Greidinger noted a timely appeal.

II

Greidinger argues that the "public disclosure" accompanying Virginia's requirement that he provide his SSN on his voter registration application unconstitutionally burdens his right to vote as protected by the First and Fourteenth Amendments. In making this argument, Greidinger attacks two components of Virginia's voter registration scheme. He objects to Virginia's permitting registered voters to obtain another registered voter's SSN via § 24.1–56, which provides that all registration books, containing all of the registration forms, "shall be opened to the inspection of any qualified voter." FN5 He also objects to § 24.1–23(8) which allows dissemination of a registered voter's SSN to a candidate for election or political party nomination, political party committee or official, incumbent office holder, and nonprofit organization which promotes voter participation and registration. FN6

FN5. In full, § 24.1–56 provides:

Books open to public inspection.

—Registration books shall be kept and preserved by the general registrar and shall be opened to the inspection of any qualified voter at the office of the registrar when the office is open for business. In addition, such book shall be available for inspection upon appointment, which appointment the general registrar shall make for all reasonable times requested. In any event, such books shall be available at additional days and times fixed by the secretary of the electoral board.

FN6. In full, § 24.1–23(8) provides:

Furnish, at a reasonable price, precinct lists for their districts to courts of the Commonwealth and the United States for jury selection purposes, to candidates for election or political party nomination to further their candidacy, political party committees or officials thereof for political purposes only, incumbent officeholders to report to their constituents; nonprofit organizations which promote voter participation and registration for that purpose only; and for no other purpose and to no one else. In addition, any general registrar whose records of registered voters are automated may furnish such lists to courts of the Commonwealth and the United States for jury selection purposes. Precinct lists shall be by printout or by magnetic tape to be used on computer equipment as may be requested.

Any person receiving such precinct lists shall take and subscribe to the following oath:

I understand that the lists requested are the property of the State Board of Elections of the Commonwealth of Virginia (or name of appropriate county or city) and I hereby affirm that I am a person

> authorized by § 24.1–23 of the Code of Virginia to receive a copy of the precinct lists described; and I further affirm that the lists will be used only for the purposes prescribed and for no other use, and that I will not permit the use or copying of such lists by persons not authorized by the Code of Virginia to obtain them.
>
> (Seal) Signature of Purchaser....

Notably, Greidinger does not challenge Virginia's receipt and internal use of his SSN. He challenges only the dissemination of the SSN to the public pursuant to § 24.1–23(8) (candidates, political parties and officials, incumbents, and nonprofit organizations which promote voter participation and voter registration) and § 24.1–56 (general public). In addition, Greidinger does not assert any constitutional right to privacy in his SSN. Rather, he argues that the privacy interest in his SSN is sufficiently strong that his right to vote cannot be predicated on the disclosure of his SSN to the public or political entities.

[1] It is axiomatic that "[n]o right is more precious in a free country than that of having a voice in the election of those who make the laws under which, as good citizens, we must live. Other rights, even the most basic, are illusory if the right to vote is undermined." *Wesberry v. Sanders*, 376 U.S. 1, 17, 84 S.Ct. 526, 535, 11 L.Ed.2d 481 (1976); *see also Yick Wo v. Hopkins*, 118 U.S. 356, 370, 6 S.Ct. 1064, 1071, 30 L.Ed. 220 (1886) (right to vote regarded as a fundamental right because it preserves all other rights); *Reynolds v. Sims*, 377 U.S. 533, 555, 84 S.Ct. 1362, 1378, 12 L.Ed.2d 506 (1964) ("[A]ny restrictions on that right [to vote] strike at the heart of representative government."). ***1349** Despite the fundamental nature of the right to vote, states may nevertheless impose certain qualifications on and regulate access to the franchise. *Lassiter v. Northampton County Bd. of Elections*, 360 U.S. 45, 50, 79 S.Ct. 985, 989, 3 L.Ed.2d 1072 (1959). Such powers have been employed to restrict the franchise in numerous contexts. *See, e.g., Marston v. Lewis*, 410 U.S. 679, 93 S.Ct. 1211, 35 L.Ed.2d 627 (1973) (residency); *Oregon v. Mitchell*, 400 U.S. 112, 91 S.Ct. 260, 27 L.Ed.2d 272 (1970) (age minimum); and *Ball v. James*, 451 U.S. 355, 101 S.Ct. 1811, 68 L.Ed.2d 150 (1981) (interested voter status). As the Supreme Court recognized in *Storer v. Brown*, 415 U.S. 724, 94 S.Ct. 1274, 39 L.Ed.2d 714 (1974):

> [A]s a practical matter, there must be a substantial regulation of elections if they are to be fair and honest and if some sort of order, rather than chaos, is to accompany the democratic processes. In any event, the States have evolved comprehensive, and in many respects complex, election codes regulating in most substantial ways, with respect to both federal and state elections, the time, place, and manner of holding primary and general elections, the registration and qualifications of voters, and the selection and qualification of candidates.

Id. at 730, 94 S.Ct. at 1279. However, the state's broad power to regulate the franchise "does not extinguish the State's responsibility to observe the limits established by the First Amendment rights of the State's citizens." *Tashjian v. Republican Party of Connecticut*, 479 U.S. 208, 217, 107 S.Ct. 544, 550, 93 L.Ed.2d 514 (1986).

The difficulty of the inquiry can best be seen through an observation the Supreme Court made almost twenty years ago in *Storer*. In assessing the validity of state election laws under the Equal Protection Clause, the Court observed:

> It is very unlikely that all or even a large portion of the state election laws would fail to pass muster under our cases; and the rule fashioned by the Court to pass on constitutional challenges to specific provisions of election laws provides no litmus-paper test for separating those restrictions that are valid from those that are invidious under the Equal Protection Clause. The rule is not self-executing and is no substitute for the hard judg-

ments that must be made. Decision in this context, as in others, is very much a matter of degree, very much a matter of consider[ing] the facts and circumstances behind the law, the interests which the State claims to be protecting, and the interests of those who are disadvantaged by the classification.

415 U.S. at 730, 94 S.Ct. at 1279 (citations and internal quotes omitted).

We must begin our inquiry by determining the proper standard to be applied to the statutes at issue. We look for guidance in cases involving voter qualifications and ballot access.[FN7] In the context of voter qualifications, traditional equal protection strict scrutiny analysis has been applied. *See Dunn v. Blumstein*, 405 U.S. 330, 336, 92 S.Ct. 995, 1000, 31 L.Ed.2d 274 (" '[B]efore that right [to vote] can be restricted, the purpose of the restriction and the assertedly overriding interest served by it must meet close constitutional scrutiny.' ") (quoting *Evans v. Cornman*, 398 U.S. 419, 422, 90 S.Ct. 1752, 1755, 26 L.Ed.2d 370 (1970)); *Hill v. Stone*, 421 U.S. 289, 297, 95 S.Ct. 1637, 1643, 44 L.Ed.2d 172 (1975) (Any restrictions other than residence, age, and citizenship must promote compelling state interests.). In applying strict scrutiny, the Supreme Court has invalidated certain measures enacted by states. *See, e.g., Harper v. Virginia Bd. of Elections*, 383 U.S. 663, 86 S.Ct. 1079, 16 L.Ed.2d 169 (1966) (right to vote predicated on $1.50 poll tax violates **1350** equal protection); *Smith v. Allwright*, 321 U.S. 649, 64 S.Ct. 757, 88 L.Ed. 987 (1944) (striking down white primary laws); *Carrington v. Rash*, 380 U.S. 89, 85 S.Ct. 775, 13 L.Ed.2d 675 (1965) (striking down on equal protection grounds statute that prevented resident military personnel from voting where stationed); and *Kramer v. Union Free School Dist. No. 15*, 395 U.S. 621, 89 S.Ct. 1886, 23 L.Ed.2d 583 (1969) (striking down statute that prevented non-property owners from voting in school district election as violative of equal protection).

FN7. The Board argues that we should ignore ballot-access precedent because we have before us a voting rights case. This argument has been categorically rejected by the Supreme Court. *See Anderson v. Celebrezze*, 460 U.S. 780, 786, 103 S.Ct. 1564, 1568, 75 L.Ed.2d 547 (1983) (" '[T]he rights of voters and the rights of candidates do not lend themselves to neat separation.' ") (quoting *Bullock v. Carter*, 405 U.S. 134, 143, 92 S.Ct. 849, 856, 31 L.Ed.2d 92 (1972)); *Williams v. Rhodes*, 393 U.S. 23, 30, 89 S.Ct. 5, 10, 21 L.Ed.2d 24 (1968) (noting associational and voting rights are "different, although overlapping, kinds of rights").

In each of these cases, the state law under attack prohibited an identified class of persons from voting. Obviously, the statutes at issue in this case do not impose such a prohibition, but rather place a burdensome condition on the exercise of the fundamental right to vote. In such cases, the Supreme Court has never clearly determined that strict scrutiny should apply. These murky waters become more lucid to the extent that the Court has distinguished between provisions that result in "an absolute denial of the franchise" and provisions that made "casting a ballot easier for some." *Kramer*, 395 U.S. at 626 n. 6, 89 S.Ct. at 1889 n. 6. For example, in upholding a state's decision not to provide absentee ballots to pretrial detainees, notwithstanding the fact that absentee ballots were available to others, the Court applied the "rational basis" test. *McDonald v. Bd. of Election Commissioners*, 394 U.S. 802, 809, 89 S.Ct. 1404, 1408, 22 L.Ed.2d 739 (1969).

The Court also applied the "rational basis" test in upholding a state law which conditioned the right to vote in a party primary on the voter's registering as a party member thirty days prior to the previous general election. This registration date was eight months prior to the presidential primary and eleven months prior to the non-presidential primary. *Rosario v. Rockefeller*, 410 U.S. 752, 93 S.Ct. 1245, 36

L.Ed.2d 1 (1973). Initially, the Court noted that the plaintiffs comprised a group of individuals who could have registered in time for the primary, but for one reason or another failed to do so. *Id.* at 755 and n. 4, 93 S.Ct. at 1248 and n. 4. The Court used this observation to distinguish those cases along the *Carrington-Dunn* line which had applied strict scrutiny. *Id.* at 757, 93 S.Ct. at 1249. The Court stated that, in the *Carrington-Dunn* line of cases, "the State [had] totally denied the electoral franchise to a particular class of residents, and there was no way in which the members of that class could have made themselves eligible to vote." *Id.* at 757, 93 S.Ct. at 1249. Comparing the statutes in the *Carrington-Dunn* line of cases to the New York statute before it, the Court stated that the New York statute "did not absolutely disenfranchise the class to which petitioners belong—newly registered voters who were eligible to enroll in a party before the previous general election." *Id.* The Court then concluded that to the extent the plaintiffs' "plight can be characterized as disenfranchisement at all, it was not caused by [the New York statute], but by their own failure to take timely steps to effect their enrollment." *Id.* at 758, 93 S.Ct. at 1250. The Court applied the "rational basis" test and upheld the statute.

The Supreme Court's continued reliance on the "absolute denial" distinction made in *Rosario* is called into question when examining recent ballot access decisions. In ballot access cases, prior to the *Anderson* decision, the Supreme Court generally applied equal protection strict scrutiny. *Williams*, 393 U.S. at 30–32, 89 S.Ct. at 10–11; *Bullock*, 405 U.S. at 142–44, 92 S.Ct. at 855–56; *Lubin v. Panish*, 415 U.S. 709, 94 S.Ct. 1315, 39 L.Ed.2d 702 (1974); *Illinois Elections Bd. v. Socialist Workers Party*, 440 U.S. 173, 99 S.Ct. 983, 59 L.Ed.2d 230 (1979); *but see, Clements v. Fashing*, 457 U.S. 957, 965–66, 102 S.Ct. 2836, 2844–45, 73 L.Ed.2d 508 (1982) (plurality opinion) ("[n]ot all ballot access restrictions require 'heightened' equal protection scrutiny").

However, in *Anderson*, the Court elected not to rest its decision on equal protection grounds, but rather directly on the First and Fourteenth Amendments. 460 U.S. at 786 n. 7, 103 S.Ct. at 1569 n. 7 ("In this case, we base our conclusions directly on *1351 the First and Fourteenth Amendments and do not engage in a separate Equal Protection Clause analysis."). *See also, Norman v. Reed*, 502 U.S. 279, —— n. 8, 112 S.Ct. 698, 705 n. 8, 116 L.Ed.2d 711 (1992) (quoting *Anderson* for the same proposition). The *Anderson* Court, however, found it helpful to rely on prior cases using the Equal Protection Clause analysis. 460 U.S. at 786 n. 7, 103 S.Ct. at 1569 n. 7 ("We rely, however, on the analysis in a number of our prior election cases resting on the Equal Protection Clause of the Fourteenth Amendment."); *Norman*, 502 U.S. at —— n. 8, 112 S.Ct. at 705 n. 8 (quoting *Anderson* for the same proposition).

In *Anderson*, the Court again recognized that determining whether a restriction is valid or invalid "cannot be resolved by any 'litmus-paper test.' " 460 U.S. at 789, 103 S.Ct. at 1570 (quoting *Storer*, 415 U.S. at 730, 94 S.Ct. at 1279). In response, the Court developed an analytical framework that amounted to a weighing of factors. This framework essentially retained the individual components of the strict scrutiny calculus:

> [A court] must first consider the character and magnitude of the asserted injury to the rights protected by the First and Fourteenth Amendments that the plaintiff seeks to vindicate. It then must identify and evaluate the precise interest put forward by the State as justifications for the burden imposed by its rule. In passing judgment, the Court must not only determine the legitimacy and the strength of each of those interests, it also must consider the extent to which those interests make it necessary to burden the plaintiff's rights. Only after weighing all these factors is the reviewing court in a position to decide whether the challenged provision is unconstitutional.
>
> *Anderson*, 460 U.S. at 789, 103 S.Ct. at 1570.

Relying on the First and Fourteenth Amendments, the Court in *Anderson* held unconstitutional an Ohio statute that required an independent candidate for President, John Anderson, to file both a statement of candidacy and a nominating petition in March in order to appear on the general election ballot in November. In assessing the character and magnitude of the asserted injury to the rights protected by the First and Fourteenth Amendments, the Court noted that the early filing deadline could have a substantial impact on independent-minded voters and candidates because the March deadline would thwart the possibility of "a newly emergent candidate [that] could serve as the focal point for a grouping of Ohio voters who decide, after mid-March, that they are dissatisfied with the choices within the two major parties." *Id.* at 791, 103 S.Ct. at 1571.

Ohio proffered three state interests that justified the restriction: (1) voter education, (2) equal treatment, and (3) political stability. *Id.* at 796, 103 S.Ct. at 1574. While the Court agreed with Ohio that it had a legitimate state interest in fostering informed and educated expression, the Court found that Ohio's interest did not justify the specific restriction at issue because the restriction had the potential to actually deprive the Ohio electorate of valuable understanding of the issues that an independent candidate could have contributed. *Id.* at 798, 103 S.Ct. at 1575. In addition, the Court in *Anderson* was neither persuaded that Ohio's interest in equal treatment was achieved by the March deadline, nor persuaded that the March deadline could be justified on the basis of Ohio's interest in political stability.

More recently, the Supreme Court ameliorated the ambiguity caused by *Anderson* with respect to the level of scrutiny to be applied when it returned to a straightforward strict scrutiny test. In *Norman*, the Court stated:

> To the degree that a State would thwart this interest by limiting the access of new parties to the ballot, we have called for the demonstration of a corresponding interest sufficiently weighty to justify this limitation, and we have accordingly required any severe restriction to be narrowly drawn to advance a state interest of compelling importance.

***1352** *Id.* 502 U.S. at ——, 112 S.Ct. at 705. (citations omitted). Similar to *Anderson*, *Norman* involved a situation in which a state had promulgated statutes making it difficult, but not impossible, for a new political party to obtain a position on the ballot. Returning to traditional strict scrutiny analysis, the Court struck two of the statutes at issue. The Court concluded that neither provision was narrowly tailored to meet the interests of Illinois. *Id.* at ——–——, 112 S.Ct. at 705–08.

[2] Similar to previous cases which employed equal protection analysis in assessing the propriety of various statutes in voter qualification and ballot access cases, *Anderson* and *Norman* recognize the precious nature of the individual and state rights at issue and the delicate balancing required to achieve electoral harmony. *Anderson* and *Norman* are also illustrative of the Supreme Court's recent focus on the degree of the burden imposed on the exercise of associational or voting rights as opposed to the "absolute denial" of associational or voting rights which the Court found critical in *Rosario*. Thus, the critical distinction between the *McDonald–Rosario* line and the *Carrington–Dunn/Anderson–Norman* lines is whether the statute at issue imposes a substantial burden on the associational rights or voting rights at stake. *Storer*, 415 U.S. at 729, 94 S.Ct. at 1278 ("substantial burdens on the right to vote or associate for political purposes are constitutionally suspect and invalid under the First and Fourteenth Amendments and under the Equal Protection Clause unless essential to serve a compelling state interest."); *Bullock*, 405 U.S. at 144, 92 S.Ct. at 856 ("Because the Texas filing-fee scheme has a real and appreciable impact on the exercise of the franchise, and because this impact is related to the resources of the voters supporting a particular candidate, we conclude, as in *Harper*, that the laws must

be 'closely scrutinized.' "). If a substantial burden exists, a common sense reading of the cases in both areas suggests that the restrictions on the right to vote must serve a compelling state interest and be narrowly tailored to serve that state interest. Generally, this is the conventional approach employed in assessing First Amendment deprivations. *Storer*, 415 U.S. at 759–62, 94 S.Ct. at 1293–95 (Brennan, J., dissenting).

A

Before we begin examining the burden on Greidinger's right to vote, we note that the Virginia statutes at issue, for all practical purposes, condition Greidinger's right to vote on the public disclosure of his SSN. Admittedly, at first glance, the disclosure of a SSN to the general public is a rather subtle price to pay to exercise the right to vote. Nevertheless, it is nothing short of a condition on the exercise of that right. To be sure, by definition, the fact that the SSN may be potentially disseminated to any registered voter or political party with the attendant possibility of a serious invasion of one's privacy is demonstrably more restrictive than predicating the right to vote on the simple receipt and internal use of the SSN. By allowing the SSN to be disseminated to registered voters or political parties upon request, Virginia's voter registration scheme conditions the right to vote on the consent to the public disclosure of a would-be voter's SSN.

B

Because Virginia's voter registration scheme conditions Greidinger's right to vote on the public disclosure of his SSN, we must examine whether this condition imposes a substantial burden.

Originated in 1936, a SSN is a nine-digit account number assigned by the Secretary of Health and Human Services for the purpose of administering the Social Security laws. *See* 42 U.S.C. § 405(c)(2)(B). SSNs were first intended for use exclusively by the federal government as a means of tracking earnings to determine the amount of Social Security taxes to credit to each worker's account. Over time, however, SSNs were permitted to be used for purposes unrelated to the administration of the Social Security system. For example in 1961, Congress authorized the Internal Revenue Service to use SSNs as taxpayer *1353 identification numbers. Pub.L. No. 87–397, 75 Stat. 828 (codified as amended at 26 U.S.C. §§ 6113, 6676).

In response to growing concerns over the accumulation of massive amounts of personal information, Congress passed the Privacy Act of 1974. This Act makes it unlawful for a governmental agency to deny a right, benefit, or privilege merely because the individual refuses to disclose his SSN. In addition, Section 7 of the Privacy Act further provides that any agency requesting an individual to disclose his SSN must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory authority such number is solicited, and what uses will be made of it." At the time of its enactment, Congress recognized the dangers of widespread use of SSNs as universal identifiers. In its report supporting the adoption of this provision, the Senate Committee stated that the widespread use of SSNs as universal identifiers in the public and private sectors is "one of the most serious manifestations of privacy concerns in the Nation." S.Rep. No. 1183, 93d Cong., 2d Sess., *reprinted in* 1974 U.S.Code Cong. & Admin. News 6916, 6943. In subsequent decisions, the Supreme Court took notice of the serious threats to privacy interests by the mass accumulation of information in computer data banks. For example, in *Whalen v. Roe*, 429 U.S. 589, 97 S.Ct. 869, 51 L.Ed.2d 64 (1977), in rejecting a privacy challenge to a New York statute that: (1) required doctors to disclose to the state information about prescriptions for certain drugs with a high potential for abuse and (2) provided for the storage of that information in a centralized computerized file, the Court observed:

> We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social secur-

ity benefits, the supervision of public health, the direction of our Armed Forces, and the enforcement of all criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures.

Id. at 605, 97 S.Ct. at 879 (footnote omitted).

Since the passage of the Privacy Act, an individual's concern over his SSN's confidentiality and misuse has become significantly more compelling. For example, armed with one's SSN, an unscrupulous individual could obtain a person's welfare benefits or Social Security benefits, order new checks at a new address on that person's checking account, obtain credit cards, or even obtain the person's paycheck. Elizabeth Neuffer, *Victims Urge Crackdown on Identity Theft*, BOSTON GLOBE, July 9, 1991, at 13, 20 (In Massachusetts, "[a]uthorities say that, with another person's Social Security number, a thief can obtain that person's welfare benefits, Social Security benefits, credit cards or even the victim's paycheck."); Michael Quint, *Bank Robbers' Latest Weapon: Social Security Numbers*, N.Y. Times, September 27, 1992, at 7 (SSN can be used to order new checks at a new address).[FN8] In California, reported cases of fraud involving the use of SSNs have increased from 390 cases in 1988 to over 800 in 1991. Y. Anwar, *Thieves Hit Social Security Numbers*, San Francisco *1354 Chronicle, August 30, 1991, A1, A2. Succinctly stated, the harm that can be inflicted from the disclosure of a SSN to an unscrupulous individual is alarming and potentially financially ruinous. These are just examples, and our review is by no means exhaustive; we highlight a few to elucidate the egregiousness of the harm.[FN9]

FN8. In greater detail, the Quint article paints a rather frightening portrait of what harm can come by the disclosure of an individual's SSN:

> For example, a Manhattan executive returned from vacation last month to a call from Citibank asking her about an unusual pattern of transactions in her accounts. Someone, armed with her Social Security number, had called the bank to request a change of address and order new checks (billed to her account, of course) and a replacement bank card.
>
> Not content with plundering the checking account, the thief, whose identity has not been determined, also sought and received approval for telephone banking, allowing money to be transferred from the executive's account to her account by telephone. Because she had been accumulating money in the savings account to pay for home renovations, the thief found a lode much larger than normal for an individual's checking account.

FN9. Other uses include unlocking the door to another's financial records, investment portfolios, school records, financial aid records, and medical records.

The degree of the burden on Greidinger's right to vote can also be seen through the case law's uniform recognition that SSNs are exempt from disclosure under Exemption 6 of the Freedom of Information Act (FOIA), 5 U.S.C. § 552(b)(6), because their disclosure would "constitute a clearly unwarranted invasion of privacy." *See, e.g., I.B.E.W. Local No. 5 v. HUD*, 852 F.2d 87, 89 (3d Cir.1988) (disclosure of SSN constituted unwarranted invasion of privacy under FOIA). Further Congressional recognition of the privacy concerns is evident from § 7 of the Privacy Act which prohibits the denial of any right, benefit, or privilege by a governmental agency because of an individual's refusal to disclose his SSN.

[3] The statutes at issue compel a would-be voter in Virginia to consent to the possibility of a profound invasion of privacy when exercising the

fundamental right to vote. As illustrated by the examples of the potential harm that the dissemination of an individual's SSN can inflict, Greidinger's decision not to provide his SSN is eminently reasonable. In other words, Greidinger's fundamental right to vote is substantially burdened to the extent the statutes at issue permit the public disclosure of his SSN.[FN10]

> FN10. Most importantly, we note that Virginia's voter registration scheme imposes a substantial burden on Greidinger's fundamental right to vote only to the extent that the scheme permits the public disclosure of his SSN. If the scheme provided for only the receipt and internal use of the SSN by Virginia, no substantial burden would exist.

C

Having identified that Greidinger's right to vote is substantially burdened by the public disclosure of his SSN, we must next determine whether Virginia has advanced a compelling state interest that justifies the disclosure and dissemination of his SSN. If Virginia advances a compelling state interest, we must determine whether disclosure of the SSN is narrowly tailored to fulfill that state interest.

[4] With respect to § 24.1–56, Virginia stipulated in the district court that it had no state interest in disseminating SSNs to private individuals. On appeal, Virginia argues that the disclosure of SSNs is a safeguard against voter fraud. With respect to § 24.1–23(8), in addition to preventing voter fraud, Virginia argues that the statute furthers Virginia's interest in promoting "participation in the electoral process." Appellee's Brief at 26. Unquestionably, Virginia has a compelling state interest in preventing voter fraud, *Storer*, 415 U.S. at 732–33, 94 S.Ct. at 1280 (state has a compelling interest in protecting the integrity of the electoral process), and promoting voter participation. However, the inquiry does not end here. We must determine whether the disclosure of the SSN under § 24.1–23(8) and/or § 24.1–56 is narrowly tailored to fulfill that state interest. We conclude that it is not.[FN11]

> FN11. Unquestionably, Virginia has a compelling state interest that is narrowly tailored in the receipt and internal use of a SSN. The internal use of SSNs assists in, among other things, identifying voter duplication and tracking felons.

Virginia's voter registration form requires a registrant to supply, among other things, his name, address, SSN, age, place of birth, and county of previous registration. Virginia's interest in preventing voter fraud and voter participation could easily be met without the disclosure of the SSN and the attendant possibility of a serious invasion of privacy that would result from that disclosure. *Accord, Pilcher v. Rains*, 853 F.2d 334, 337 (5th Cir.1988) (requirement that voters signing ballot access petition supply "voter registration number" not necessary to distinguish among voters sharing common names).[FN12] Most assuredly,*1355 an address or date of birth would sufficiently distinguish among voters that shared a common name. Moreover, the same state interest could be achieved through the use of a voter registration number as opposed to a SSN. Following this tack, Virginia would derive the same benefits as the disclosure of a SSN. Thus, to the extent § 24.1–23(8) and § 24.1–56 allow Virginia's voter registration scheme to "sweep [ ] broader than necessary to advance electoral order," *Normal*, 502 U.S. at ——, 112 S.Ct. at 706, it creates an intolerable burden on Greidinger's fundamental right to vote.

> FN12. Interestingly, the Board never explains how the disclosure of SSNs to political parties furthers Virginia's interest in electoral participation. More to the point, the Board never explains why a SSN is more necessary to further voter participation than the name, address, date of birth, and other voter registration information already provided.

III

In summary, we hold to the extent that § 24.1–23(8) and/or § 24.1–56 permit the public disclosure of Greidinger's SSN as a condition of his right to vote, it creates an intolerable burden on that right as protected by the First and Fourteenth Amendments. Accordingly, the judgment of the district court is reversed. We remand the case to the district court to give the Commonwealth of Virginia the responsibility to cure this constitutional infirmity by either deleting the requirement that a registrant disclose his SSN or eliminating the use of SSNs in voter registration records open to public inspection and contained in voter registration lists provided to candidates for election, political party committees and officials, incumbent office holders, and non-profit organizations which promote voter participation and registration. We also remand the case for further proceedings on the Privacy Act notice, which will have to be revised in light of our decision, and the issue of attorneys' fees.[FN13]

FN13. In light of our decision, we believe it is unwise to review the district court's determination on the issue of attorneys' fees at this time.

REVERSED AND REMANDED FOR FURTHER PROCEEDINGS.

C.A.4 (Va.),1993.
Greidinger v. Davis
988 F.2d 1344, 61 USLW 2585, Unempl.Ins.Rep. (CCH) P 17193A

END OF DOCUMENT

Republic of the Philippines
SUPREME COURT
Manila

EN BANC

G.R. No. 127685 July 23, 1998

BLAS F. OPLE, petitioner,

vs.

RUBEN D. TORRES, ALEXANDER AGUIRRE, HECTOR VILLANUEVA, CIELITO HABITO, ROBERT BARBERS, CARMENCITA REODICA, CESAR SARINO, RENATO VALENCIA, TOMAS P. AFRICA, HEAD OF THE NATIONAL COMPUTER CENTER and CHAIRMAN OF THE COMMISSION ON AUDIT, respondents.

PUNO, *J.:*

The petition at bar is a commendable effort on the part of Senator Blas F. Ople to prevent the shrinking of the right to privacy, which the revered Mr. Justice Brandeis considered as "the most comprehensive of rights and the right most valued by civilized men." [1] Petitioner Ople prays that we invalidate Administrative Order No. 308 entitled "Adoption of a National Computerized Identification Reference System" on two important constitutional grounds, *viz*: one, it is a usurpation of the power of Congress to legislate, and two, it impermissibly intrudes on our citizenry's protected zone of privacy. We grant the petition for the rights sought to be vindicated by the petitioner need stronger barriers against further erosion.

A.O. No. 308 was issued by President Fidel V. Ramos On December 12, 1996 and reads as follows:

ADOPTION OF A NATIONAL COMPUTERIZED

IDENTIFICATION REFERENCE SYSTEM

WHEREAS, there is a need to provide Filipino citizens and foreign residents with the facility to conveniently transact business with basic service and social security providers and other government instrumentalities;

WHEREAS, this will require a computerized system to properly and efficiently identify persons seeking basic services on social security and reduce, if not totally eradicate fraudulent transactions and misrepresentations;

WHEREAS, a concerted and collaborative effort among the various basic services and social security providing agencies and other government intrumentalities is required to achieve such a system;

NOW, THEREFORE, I, FIDEL V. RAMOS, President of the Republic of the Philippines, by virtue of the powers vested in me by law, do hereby direct the following:

Sec. 1. *Establishment of a National Compoterized Identification Reference System.* A decentralized Identification Reference System among the key basic services and social security providers is hereby established.

Sec. 2. *Inter-Agency Coordinating Committee.* An Inter-Agency Coordinating Committee (IACC) to draw-up the implementing guidelines and oversee the implementation of the System is hereby created, chaired by the Executive Secretary, with the following as members:

Head, Presidential Management Staff

Secretary, National Economic Development Authority

Secretary, Department of the Interior and Local Government

Secretary, Department of Health

Administrator, Government Service Insurance System,

Administrator, Social Security System,

Administrator, National Statistics Office

Managing Director, National Computer Center.

Sec. 3. *Secretariat.* The National Computer Center (NCC) is hereby designated as secretariat to the IACC and as such shall provide administrative and technical support to the IACC.

Sec. 4. *Linkage Among Agencies.* The Population Reference Number (PRN) generated by the NSO shall serve as the common reference number to establish a linkage among concerned agencies. The IACC Secretariat shall coordinate with the different Social Security and Services Agencies to establish the standards in the use of Biometrics Technology and in computer application designs of their respective systems.

Sec. 5. *Conduct of Information Dissemination Campaign.* The Office of the Press Secretary, in coordination with the National Statistics Office, the GSIS and SSS as lead agencies and other concerned agencies shall undertake a massive tri-media information dissemination campaign to educate and raise public awareness on the importance and use of the PRN and the Social Security Identification Reference.

Sec. 6. *Funding.* The funds necessary for the implementation of the system shall be sourced from the respective budgets of the concerned agencies.

Sec. 7. *Submission of Regular Reports.* The NSO, GSIS and SSS shall submit regular reports to the Office of the President through the IACC, on the status of implementation of this undertaking.

Sec. 8. *Effectivity.* This Administrative Order shall take effect immediately.

DONE in the City of Manila, this 12th day of December in the year of Our Lord, Nineteen Hundred and Ninety-Six.

(SGD.) FIDEL V. RAMOS

A.O. No. 308 was published in four newspapers of general circulation on January 22, 1997 and January 23, 1997. On January 24, 1997, petitioner filed the instant petition against respondents, then Executive Secretary Ruben Torres and the heads of the government agencies, who as members of the Inter-Agency Coordinating Committee, are charged with the implementation of A.O. No. 308. On April 8, 1997, we issued a temporary restraining order enjoining its implementation.

Petitioner contends:

A. THE ESTABLISNMENT OF A NATIONAL COMPUTERIZED IDENTIFICATION REFERENCE SYSTEM REQUIRES A LEGISLATIVE ACT. THE ISSUANCE OF A.O. NO. 308 BY THE PRESIDENT OF THE REPUBLIC OF THE PHILIPPINES IS, THEREFORE, AN UNCONSTITUTIONAL USURPATION OF THE LEGISLATIVE POWERS OF THE CONGRESS OF THE REPUBLIC OF THE PHILIPPINES.

B. THE APPROPRIATION OF PUBLIC FUNDS BY THE PRESIDENT FOR THE IMPLEMENTATION OF A.O. NO. 308 IS AN UNCONSTITUTIONAL USURPATION OF THE EXCLUSIVE RIGHT OF CONGRESS TO APPROPRIATE PUBLIC FUNDS FOR EXPENDITURE.

C. THE IMPLEMENTATION OF A.O. NO. 308 INSIDIOUSLY LAYS THE GROUNDWORK FOR A SYSTEM WHICH WILL VIOLATE THE BILL OF RIGHTS ENSHRINED IN THE CONSTITUTION. [2]

Respondents counter-argue:

A. THE INSTANT PETITION IS NOT A JUSTICIABLE CASE AS WOULD WARRANT A JUDICIAL REVIEW;

B. A.O. NO. 308 [1996] WAS ISSUED WITHIN THE EXECUTIVE AND ADMINISTRATIVE POWERS OF THE PRESIDENT WITHOUT ENCROACHING ON THE LEGISLATIVE POWERS OF CONGRESS;

C. THE FUNDS NECESSARY FOR THE IMPLEMENTATION OF THE IDENTIFICATION REFERENCE SYSTEM MAY BE SOURCED FROM THE BUDGETS OF THE CONCERNED AGENCIES;

D. A.O. NO. 308 [1996] PROTECTS AN INDIVIDUAL'S INTEREST IN PRIVACY. [3]

We now resolve.

I

As is usual in constitutional litigation, respondents raise the threshold issues relating to the standing to sue of the petitioner and the justiciability of the case at bar. More specifically, respondents aver that petitioner has no legal interest to uphold and that the implementing rules of A.O. No. 308 have yet to be promulgated.

These submissions do not deserve our sympathetic ear. Petitioner Ople is a distinguished member of our Senate. As a Senator, petitioner is possessed of the requisite standing to bring suit raising the issue that the issuance of A.O. No. 308 is a usurpation of legislative power. [4] As taxpayer and member of the Government Service Insurance System (GSIS), petitioner can also impugn the legality of the misalignment of public funds and the misuse of GSIS funds to implement A.O. No. 308. [5]

The ripeness for adjudication of the Petition at bar is not affected by the fact that the implementing rules of A.O. No. 308 have yet to be promulgated. Petitioner Ople assails A.O. No. 308 as invalid *per se* and as infirmed on its face. His action is not premature for the rules yet to be promulgated cannot cure its fatal defects. Moreover, the respondents themselves have started the implementation of A.O. No. 308 without waiting for the rules. As early as January 19, 1997, respondent Social Security System (SSS) caused the publication of a notice to bid for the manufacture of the National Identification (ID) card. [6] Respondent Executive Secretary Torres has publicly announced that representatives from the GSIS and the SSS have completed the guidelines for the national identification system. [7] All signals from the respondents show their unswerving will to implement A.O. No. 308 and we need not wait for the formality of the rules to pass judgment on its constitutionality. In this light, the dissenters insistence that we tighten the rule on standing is not a commendable stance as its result would be to throttle an important constitutional principle and a fundamental right.

II

We now come to the core issues. Petitioner claims that A.O. No. 308 is not a mere administrative order but a law and hence, beyond the power of the President to issue. He alleges that A.O. No. 308 establishes a system of identification that is all-encompassing in scope, affects the life and liberty of every Filipino citizen and foreign resident, and more particularly, violates their right to privacy.

Petitioner's sedulous concern for the Executive not to trespass on the lawmaking domain of Congress is understandable. The blurring of the demarcation line between the power of the Legislature to make laws and the power of the Executive to execute laws will disturb their delicate balance of power and cannot be allowed. Hence, the exercise by one branch of government of power belonging to another will be given a stricter scrutiny by this Court.

The line that delineates Legislative and Executive power is not indistinct. Legislative power is "the authority, under the Constitution, to make laws, and to alter and repeal them." [8] The Constitution, as the will of the people in their original, sovereign and unlimited capacity, has vested this power in the Congress of the Philippines. [9] The grant of legislative power to Congress is broad, general and comprehensive. [10] The legislative body possesses plenary power for all purposes of civil government. [11] Any power, deemed to be legislative by usage and tradition, is necessarily possessed by Congress, unless the Constitution has lodged it elsewhere. [12] In fine, except as limited by the Constitution, either expressly or impliedly, legislative power embraces all subjects and extends to matters of general concern or common interest. [13]

While Congress is vested with the power to enact laws, the President executes the laws. [14] The executive power is vested in the Presidents. [15] It is generally defined as the power to enforce and administer the laws. [16] It is the power of carrying the laws into practical operation and enforcing their due observance. [17]

As head of the Executive Department, the President is the Chief Executive. He represents the government as a whole and sees to it that all laws are enforced by the officials and employees of his department. [18] He has control over the executive department, bureaus and offices. This means that he has the authority to assume directly the functions of the executive department, bureau and office or interfere with the discretion of its officials. [19] Corollary to the power of control, the President also has the duty of supervising the enforcement of laws for the maintenance of general peace and public order. Thus, he is granted administrative power over bureaus and offices under his control to enable him to discharge his duties effectively. [20]

Administrative power is concerned with the work of applying policies and enforcing orders as determined by proper

governmental organs. [21] It enables the President to fix a uniform standard of administrative efficiency and check the official conduct of his agents. [22] To this end, he can issue administrative orders, rules and regulations.

Prescinding from these precepts, we hold that A.O. No. 308 involves a subject that is not appropriate to be covered by an administrative order. An administrative order is:

> Sec. 3. *Administrative Orders.* — Acts of the President which relate to particular aspects of governmental operation in pursuance of his duties as administrative head shall be promulgated in administrative orders. [23]

An administrative order is an ordinance issued by the President which relates to specific aspects in the administrative operation of government. It must be in harmony with the law and should be for the sole purpose of implementing the law and carrying out the legislative policy. [24] We reject the argument that A.O. No. 308 implements the legislative policy of the Administrative Code of 1987. The Code is a general law and "incorporates in a unified document the major structural, functional and procedural principles of governance." [25] and "embodies changes in administrative structure and procedures designed to serve the people." [26] The Code is divided into seven (7) Books: Book I deals with Sovereignty and General Administration, Book II with the Distribution of Powers of the three branches of Government, Book III on the Office of the President, Book IV on the Executive Branch, Book V on Constitutional Commissions, Book VI on National Government Budgeting, and Book VII on Administrative Procedure. These Books contain provisions on the organization, powers and general administration of the executive, legislative and judicial branches of government, the organization and administration of departments, bureaus and offices under the executive branch, the organization and functions of the Constitutional Commissions and other constitutional bodies, the rules on the national government budget, as well as guideline for the exercise by administrative agencies of quasi-legislative and quasi-judicial powers. The Code covers both the internal administration of government, *i.e*, internal organization, personnel and recruitment, supervision and discipline, and the effects of the functions performed by administrative officials on private individuals or parties outside government. [27]

It cannot be simplistically argued that A.O. No. 308 merely implements the Administrative Code of 1987. It establishes for the first time a National Computerized Identification Reference System. Such a System requires a delicate adjustment of various contending state policies — the primacy of national security, the extent of privacy interest against dossier-gathering by government, the choice of policies, etc. Indeed, the dissent of Mr. Justice Mendoza states that the A.O. No. 308 involves the all-important freedom of thought. As said administrative order redefines the parameters of some basic rights of our citizenry *vis-a-vis* the State as well as the line that separates the administrative power of the President to make rules and the legislative power of Congress, it ought to be evident that it deals with a subject that should be covered by law.

Nor is it correct to argue as the dissenters do that A.D. No. 308 is not a law because it confers no right, imposes no duty, affords no proclection, and creates no office. Under A.O. No. 308, a citizen cannot transact business with government agencies delivering basic services to the people without the contemplated identification card. No citizen will refuse to get this identification card for no one can avoid dealing with government. It is thus clear as daylight that without the ID, a citizen will have difficulty exercising his rights and enjoying his privileges. Given this reality, the contention that A.O. No. 308 gives no right and imposes no duty cannot stand.

Again, with due respect, the dissenting opinions unduly expand the limits of administrative legislation and consequently erodes the plenary power of Congress to make laws. This is contrary to the established approach defining the traditional limits of administrative legislation. As well stated by Fisher: ". . . Many regulations however, bear directly on the public. It is here that administrative legislation must he restricted in its scope and application. Regulations are not supposed to be a substitute for the general policy-making that Congress enacts in the form of a public law. Although administrative regulations are entitled to respect, the authority to prescribe rules and regulations is not an independent source of power to make laws." [28]

III

Assuming, arguendo, that A.O. No. 308 need not be the subject of a law, still it cannot pass constitutional muster as an administrative legislation because facially it violates the right to privacy. The essence of privacy is the "right to be let alone." [29] In the 1965 case of Griswold v. Connecticut, [30] the United States Supreme Court gave more substance to the right of privacy when it ruled that the right has a constitutional foundation. It held that there is a right of privacy which can be found within the penumbras of the First, Third, Fourth, Fifth and Ninth Amendments, [31] *viz*:

> Specific guarantees in the Bill of Rights have penumbras formed by emanations from these guarantees that help give them life and substance . . . various guarantees create zones of privacy. The right of association contained in the penumbra of the First Amendment is one, as we have seen. The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the

> "right of the people to be secure in their persons, houses and effects, against unreasonable searches and seizures." The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which government may not force him to surrender to his detriment. The Ninth Amendment provides: "The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."

In the 1968 case of *Morfe v. Mutuc*, [32] we adopted the Griswold ruling that there is a constitutional right to privacy. Speaking thru Mr. Justice, later Chief Justice, Enrique Fernando, we held:

> xxx xxx xxx
>
> The Griswold case invalidated a Connecticut statute which made the use of contraceptives a criminal offence on the ground of its amounting to an unconstitutional invasion of the right of privacy of married persons; rightfully it stressed "a relationship lying within the zone of privacy created by several fundamental constitutional guarantees." It has wider implications though. The constitutional right to privacy has come into its own.
>
> So it is likewise in our jurisdiction. The right to privacy as such is accorded recognition independently of its identification with liberty; in itself, it is fully deserving of constitutional protection. The language of Prof. Emerson is particularly apt: "The concept of limited government has always included the idea that governmental powers stop short of certain intrusions into the personal life of the citizen. This is indeed one of the basic distinctions between absolute and limited government. Ultimate and pervasive control of the individual, in all aspects of his life, is the hallmark of the absolute state. In contrast, a system of limited government safeguards a private sector, which belongs to the individual, firmly distinguishing it from the public sector, which the state can control. Protection of this private sector — protection, in other words, of the dignity and integrity of the individual — has become increasingly important as modern society has developed. All the forces of a technological age — industrialization, urbanization, and organization — operate to narrow the area of privacy and facilitate intrusion into it. In modern terms, the capacity to maintain and support this enclave of private life marks the difference between a democratic and a totalitarian society."

Indeed, if we extend our judicial gaze we will find that the right of privacy is recognized and enshrined in several provisions of our Constitution. [33] It is expressly recognized in section 3 (1) of the Bill of Rights:

> Sec. 3. (1) The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law.

Other facets of the right to privacy are protectad in various provisions of the Bill of Rights, *viz*: [34]

> Sec. 1. No person shall be deprived of life, liberty, or property without due process of law, nor shall any person be denied the equal protection of the laws.
>
> Sec. 2. The right of the people to be secure in their persons, houses papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.
>
> xxx xxx xxx
>
> Sec. 6. The liberty of abode and of changing the same within the limits prescribed by law shall not be impaired except upon lawful order of the court. Neither shall the right to travel be impaired except in the interest of national security, public safety, or public health as may be provided by law.
>
> xxx xxx xxx
>
> Sec. 8. The right of the people, including those employed in the public and private sectors, to form unions, associations, or societies for purposes not contrary to law shall not be abridged.
>
> Sec. 17. No person shall be compelled to be a witness against himself.

Zones of privacy are likewise recognized and protected in our laws. The Civil Code provides that "[e]very person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons" and punishes as actionable torts several acts by a person of meddling and prying into the privacy of another. [35] It also holds a public officer or employee or any private individual liable for damages for any violation of the rights and liberties of another

person, [36] and recognizes the privacy of letters and other private communications. [37] The Revised Penal Code makes a crime the violation of secrets by an officer, [38] the revelation of trade and industrial secrets, [39] and trespass to dwelling. [40] Invasion of privacy is an offense in special laws like the Anti-Wiretapping Law, [41] the Secrecy of Bank Deposits Act [42] and the Intellectual Property Code. [43] The Rules of Court on privileged communication likewise recognize the privacy of certain information. [44]

Unlike the dissenters, we prescind from the premise that the right to privacy is a fundamental right guaranteed by the Constitution, hence, it is the burden of government to show that A.O. No. 308 is justified by some compelling state interest and that it is narrowly drawn. A.O. No. 308 is predicated on two considerations: (1) the need to provides our citizens and foreigners with the facility to conveniently transact business with basic service and social security providers and other government instrumentalities and (2) the need to reduce, if not totally eradicate, fraudulent transactions and misrepresentations by persons seeking basic services. It is debatable whether these interests are compelling enough to warrant the issuance of A.O. No. 308. But what is not arguable is the broadness, the vagueness, the overbreadth of A.O. No. 308 which if implemented will put our people's right to privacy in clear and present danger.

The heart of A.O. No. 308 lies in its Section 4 which provides for a Population Reference Number (PRN) as a "common reference number to establish a linkage among concerned agencies" through the use of "Biometrics Technology" and "computer application designs."

Biometry or biometrics is "the science of the applicatin of statistical methods to biological facts; a mathematical analysis of biological data." [45] The term "biometrics" has evolved into a broad category of technologies which provide precise confirmation of an individual's identity through the use of the individual's own physiological and behavioral characteristics. [46] A physiological characteristic is a relatively stable physical characteristic such as a fingerprint, retinal scan, hand geometry or facial features. A behavioral characteristic is influenced by the individual's personality and includes voice print, signature and keystroke. [47] Most biometric idenfication systems use a card or personal identificatin number (PIN) for initial identification. The biometric measurement is used to verify that the individual holding the card or entering the PIN is the legitimate owner of the card or PIN. [48]

A most common form of biological encoding is finger-scanning where technology scans a fingertip and turns the unique pattern therein into an individual number which is called a biocrypt. The biocrypt is stored in computer data banks [49] and becomes a means of identifying an individual using a service. This technology requires one's fingertip to be scanned every time service or access is provided. [50] Another method is the retinal scan. Retinal scan technology employs optical technology to map the capillary pattern of the retina of the eye. This technology produces a unique print similar to a finger print. [51] Another biometric method is known as the "artificial nose." This device chemically analyzes the unique combination of substances excreted from the skin of people. [52] The latest on the list of biometric achievements is the thermogram. Scientists have found that by taking pictures of a face using infra-red cameras, a unique heat distribution pattern is seen. The different densities of bone, skin, fat and blood vessels all contribute to the individual's personal "heat signature." [53]

In the last few decades, technology has progressed at a galloping rate. Some science fictions are now science facts. Today, biometrics is no longer limited to the use of fingerprint to identify an individual. It is a new science that uses various technologies in encoding any and all biological characteristics of an individual for identification. It is noteworthy that A.O. No. 308 does not state what specific biological characteristics and what particular biometrics technology shall be used to identify people who will seek its coverage. Considering the banquest of options available to the implementors of A.O. No. 308, the fear that it threatens the right to privacy of our people is not groundless.

A.O. No. 308 should also raise our antennas for a further look will show that it does not state whether encoding of data is limited to biological information alone for identification purposes. In fact, the Solicitor General claims that the adoption of the Identification Reference System will contribute to the "generation of population data for development planning." [54] This is an admission that the PRN will not be used solely for identification but the generation of other data with remote relation to the avowed purposes of A.O. No. 308. Clearly, the indefiniteness of A.O. No. 308 can give the government the roving authority to store and retrieve information for a purpose other than the identification of the individual through his PRN.

The potential for misuse of the data to be gathered under A.O. No. 308 cannot be undarplayed as the dissenters do. Pursuant to said administrative order, an individual must present his PRN everytime he deals with a government agency to avail of basic services and security. His transactions with the government agency will necessarily be recorded — whether it be in the computer or in the documentary file of the agency. The individual's file may include his transactions for loan availments, income tax returns, statement of assets and liabilities, reimbursements for medication, hospitalization, etc. The more frequent the use of the PRN, the better the chance of building a huge formidable informatin base through the electronic linkage of the files. [55] The data may be gathered for gainful and useful government purposes; but the existence of this vast reservoir of personal information constitutes a covert invitation to

misuse, a temptation that may be too great for some of our authorities to resist. [56]

We can even grant, arguendo, that the computer data file will be limited to the name, address and other basic personal infomation about the individual. [57] Even that hospitable assumption will not save A.O. No. 308 from constitutional infirmity for again said order does not tell us in clear and categorical terms how these information gathered shall he handled. It does not provide who shall control and access the data, under what circumstances and for what purpose. These factors are essential to safeguard the privacy and guaranty the integrity of the information. [58] Well to note, the computer linkage gives other government agencies access to the information. Yet, there are no controls to guard against leakage of information. When the access code of the control programs of the particular computer system is broken, an intruder, without fear of sanction or penalty, can make use of the data for whatever purpose, or worse, manipulate the data stored within the system. [59]

It is plain and we hold that A.O. No. 308 falls short of assuring that personal information which will be gathered about our people will only be processed for unequivocally specified purposes. [60] The lack of proper safeguards in this regard of A.O. No. 308 may interfere with the individual's liberty of abode and travel by enabling authorities to track down his movement; it may also enable unscrupulous persons to access confidential information and circumvent the right against self-incrimination; it may pave the way for "fishing expeditions" by government authorities and evade the right against unreasonable searches and seizures. [61] The possibilities of abuse and misuse of the PRN, biometrics and computer technology are accentuated when we consider that the individual lacks control over what can be read or placed on his ID, much less verify the correctness of the data encoded. [62] They threaten the very abuses that the Bill of Rights seeks to prevent. [63]

The ability of sophisticated data center to generate a comprehensive cradle-to-grave dossier on an individual and transmit it over a national network is one of the most graphic threats of the computer revolution. [64] The computer is capable of producing a comprehensive dossier on individuals out of information given at different times and for varied purposes. [65] It can continue adding to the stored data and keeping the information up to date. Retrieval of stored date is simple. When information of a privileged character finds its way into the computer, it can be extracted together with other data on the subject. [66] Once extracted, the information is putty in the hands of any person. The end of privacy begins.

Though A.O. No. 308 is undoubtedly not narrowly drawn, the dissenting opinions would dismiss its danger to the right to privacy as speculative and hypothetical. Again, we cannot countenance such a laidback posture. The Court will not be true to its role as the ultimate guardian of the people's liberty if it would not immediately smother the sparks that endanger their rights but would rather wait for the fire that could consume them.

We reject the argument of the Solicitor General that an individual has a reasonable expectation of privacy with regard to the Natioal ID and the use of biometrics technology as it stands on quicksand. The reasonableness of a person's expectation of privacy depends on a two-part test: (1) whether by his conduct, the individual has exhibited an expectation of privacy; and (2) whether this expectation is one that society recognizes as reasonable. [67] The factual circumstances of the case determines the reasonableness of the expectation. [68] However, other factors, such as customs, physical surroundings and practices of a particular activity, may serve to create or diminish this expectation. [69] The use of biometrics and computer technology in A.O. No. 308 does not assure the individual of a reasonable expectation of privacy. [70] As technology advances, the level of reasonably expected privacy decreases. [71] The measure of protection granted by the reasonable expectation diminishes as relevant technology becomes more widely accepted. [72] The security of the computer data file depends not only on the physical inaccessibility of the file but also on the advances in hardware and software computer technology. A.O. No. 308 is so widely drawn that a minimum standard for a reasonable expectation of privacy, regardless of technology used, cannot be inferred from its provisions.

The rules and regulations to be by the IACC cannot remedy this fatal defect. Rules and regulations merely implement the policy of the law or order. On its face, A.O. No. gives the IACC virtually infettered discretion to determine the metes and bounds of the ID System.

Nor do your present laws prvide adequate safeguards for a reasonable expectation of privacy. Commonwealth Act. No. 591 penalizes the disclosure by any person of data furnished by the individual to the NSO with imprisonment and fine. [73] Republic Act. No. 1161 prohibits public disclosure of SSS employment records and reports. [74] These laws, however, apply to records and data with the NSO and the SSS. It is not clear whether they may be applied to data with the other government agencies forming part of the National ID System. The need to clarify the penal aspect of A.O. No. 308 is another reason why its enactment should be given to Congress.

Next, the Solicitor General urges us to validate A.O. No. 308's abridgment of the right of privacy by using the rational relationship test. [75] He stressed that the purposes of A.O. No. 308 are: (1) to streamline and speed up the implementation of basic government services, (2) eradicate fraud by avoiding duplication of services, and (3) generate population data for development planning. He cocludes that these purposes justify the incursions into the right to privacy for the means are rationally related to the end. [76]

We are not impressed by the argument. In *Morfe v. Mutuc*, [77] we upheld the constitutionality of R.A. 3019, the Anti-Graft and Corrupt Practices Act, as a valid police power measure. We declared that the law, in compelling a public officer to make an annual report disclosing his assets and liabilities, his sources of income and expenses, did not infringe on the individual's right to privacy. The law was enacted to promote morality in public administration by curtailing and minimizing the opportunities for official corruption and maintaining a standard of honesty in the public service. [78]

The same circumstances do not obtain in the case at bar. For one, R.A. 3019 is a statute, not an administrative order. Secondly, R.A. 3019 itself is sufficiently detailed. The law is clear on what practices were prohibited and penalized, and it was narrowly drawn to avoid abuses. IN the case at bar, A.O. No. 308 may have been impelled by a worthy purpose, but, it cannot pass constitutional scrutiny for it is not narrowly drawn. And we now hod that when the integrity of a fundamental right is at stake, this court will give the challenged law, administrative order, rule or regulation a stricter scrutiny. It will not do for the authorities to invoke the presumption of regularity in the performance of official duties. Nor is it enough for the authorities to prove that their act is not irrational for a basic right can be diminished, if not defeated, even when the government does not act irrationally. They must satisfactorily show the presence of compelling state interests and that the law, rule or regulation is narrowly drawn to preclude abuses. This approach is demanded by the 1987 Constitution whose entire matrix is designed to protect human rights and to prevent authoritarianism. In case of doubt, the least we can do is to lean towards the stance that will not put in danger the rights protected by the Constitutions.

The case of *Whalen v. Roe* [79] *cited* by the Solicilor General is also off-line. In Whalen, the United States Supreme Court was presented with the question of whether the State of New York could keep a centralized computer record of the names and addresses of all persons who obtained certain drugs pursuant to a doctor's prescription. The New York State Controlled Substance Act of 1972 required physicians to identify parties obtaining prescription drugs enumerated in the statute, *i.e.*, drugs with a recognized medical use but with a potential for abuse, so that the names and addresses of the patients can be recorded in a centralized computer file of the State Department of Health. The plaintiffs, who were patients and doctors, claimed that some people might decline necessary medication because of their fear that the computerized data may be readily available and open to public disclosure; and that once disclosed, it may stigmatize them as drug addicts. [80] The plaintiffs alleged that the statute invaded a constitutionally protected zone of privacy, *i.e.*, the individual interest in avoiding disclosure of personal matters, and the interest in independence in making certain kinds of important decisions. The U.S. Supreme Court held that while an individual's interest in avoiding disclosuer of personal matter is an aspect of the right to privacy, the statute did not pose a grievous threat to establish a constitutional violation. The Court found that the statute was necessary to aid in the enforcement of laws designed to minimize the misuse of dangerous drugs. The patient-identification requirement was a product of an orderly and rational legislative decision made upon recommmendation by a specially appointed commission which held extensive hearings on the matter. Moreover, the statute was narrowly drawn and contained numerous safeguards against indiscriminate disclosure. The statute laid down the procedure and requirements for the gathering, storage and retrieval of the informatin. It eburnerated who were authorized to access the data. It also prohibited public disclosure of the data by imposing penalties for its violation. In view of these safeguards, the infringement of the patients' right to privacy was justified by a valid exercise of police power. As we discussed above, A.O. No. 308 lacks these vital safeguards.

Even while we strike down A.O. No. 308, we spell out in neon that the Court is not *per se* agains the use of computers to accumulate, store, process, retvieve and transmit data to improve our bureaucracy. Computers work wonders to achieve the efficiency which both government and private industry seek. Many information system in different countries make use of the computer to facilitate important social objective, such as better law enforcement, faster delivery of public services, more efficient management of credit and insurance programs, improvement of telecommunications and streamlining of financial activities. [81] Used wisely, data stored in the computer could help good administration by making accurate and comprehensive information for those who have to frame policy and make key decisions. [82] The benefits of the computer has revolutionized information technology. It developed the internet, [83] introduced the concept of cyberspace [84] and the information superhighway where the individual, armed only with his personal computer, may surf and search all kinds and classes of information from libraries and databases connected to the net.

In no uncertain terms, we also underscore that the right to privacy does not bar all incursions into individual privacy. The right is not intended to stifle scientific and technological advancements that enhance public service and the common good. It merely requires that the law be narrowly focused [85] and a compelling interest justify such intrusions. [86] Intrusions into the right must be accompanied by proper safeguards and well-defined standards to prevent unconstitutional invasions. We reiterate that any law or order that invades individual privacy will be subjected by this Court to strict scrutiny. The reason for this stance was laid down in *Morfe v. Mutuc*, to wit:

> The concept of limited government has always included the idea that governmental powers stop short of certain intrusions into the personal life of the citizen. This is indeed one of the basic disctinctions between absolute and limited government. Ultimate and pervasive control of the individual, in all aspects of his life, is the hallmark of the absolute state. In contrast, a system of limited government safeguards a private sector, which belongs to the individual, firmly distinguishing it from the public sector, which the state can control. Protection of this private sector — protection, in other words, of the dignity and integrity of the individual — has become increasingly important as modern society has developed. All the forces of a technological age — industrialization, urbanization, and organization —

operate to narrow the area of privacy and facilitate intrusion into it. In modern terms, the capacity to maintain and support this enclave of private life marks the difference between a democratic and a totalitarian society. [87]

IV

The right to privacy is one of the most threatened rights of man living in a mass society. The threats emanate from various sources — governments, journalists, employers, social scientists, etc. [88] In th case at bar, the threat comes from the executive branch of government which by issuing A.O. No. 308 pressures the people to surrender their privacy by giving information about themselves on the pretext that it will facilitate delivery of basic services. Given the record-keeping power of the computer, only the indifferent fail to perceive the danger that A.O. No. 308 gives the government the power to compile a devastating dossier against unsuspecting citizens. It is timely to take note of the well-worded warning of Kalvin, Jr., "the disturbing result could be that everyone will live burdened by an unerasable record of his past and his limitations. In a way, the threat is that because of its record-keeping, the society will have lost its benign capacity to forget." [89] Oblivious to this counsel, the dissents still say we should not be too quick in labelling the right to privacy as a fundamental right. We close with the statement that the right to privacy was not engraved in our Constitution for flattery.

IN VIEW WHEREOF, the petition is granted and Adminisrative Order No. 308 entitled "Adoption of a National Computerized Identification Reference System" declared null and void for being unconstitutional.

SO ORDERED.

Bellosillo and Martinez, JJ., concur.

Narvasa, C.J., I join Justices Kapunan and Mendoza in their dissents.

Regalado, J., In the result.

Davide, Jr., In the result and I join Mr. Justice Panganiban in his separate opinion.

Romero, J., Please see separate opinion.

Melo, J., I join the dissents of Justices Kapunan and Mendoza.

Vitug, J., See separate opinion.

Kapunan, J., See dissenting opinion.

Mendoza, J., Please see dissenting opinion.

Panganiban, J., Please see Separate Opinion.

Quisumbing, J., I join in dissenting opinion of JJ. Mendoza and Kapunan.

Purisima, J., I join in Justice Mendoza's dissenting.

Separate Opinions

ROMERO, J., separate opinion;

What marks offs man from a beast?

Aside from the distinguishing physical characteristics, man is a rational being, one who is endowed with intellect which allows him to apply reasoned judgment to problems at hand; he has the innate spiritual faculty which can tell, not only what is right but, as well, what is moral and ethical. Because of his sensibilities, emotions and feelings, he likewise possesses a sense of shame. In varying degrees as dictated by diverse cultures, he erects a wall between himself and the outside world wherein he can retreat in solitude, protecting himself from prying eyes and ears and their extensions, whether form individuals, or much later, from authoritarian intrusions.

Piercing through the mists of time, we find the original Man and Woman defying the injunction of God by eating of

the forbidden fruit in the Garden. And when their eyes were "opened" forthwith "they sewed fig leaves together, and made themselves aprons." [1] Down the corridors of time, we find man fashioning "fig leaves" of sorts or setting up figurative walls, the better to insulate themselves from the rest of humanity.

Such vague stirrings of the desire "to be left alone," considered "anti-social" by some, led to the development of the concept of "privacy," unheard of among beasts. Different branches of science, have made their own studies of this craving of the human spirit — psychological, anthropological sociological and philosophical, with the legal finally giving its imprimatur by elevating it to the status ofa right, specifically a private right.

Initially recognized as an aspect of tort law, it created giant waves in legal circles with the publication in the Harvard Law Review [2] of the trail-blazing article, "The Right to Privacy," by Samuel D. Warren and Louis D. Brandeis.

Whether viewed as a personal or a property right, it found its way in Philippine Constitutions and statutes; this, in spite of the fact that Philippine culture can hardly be said to provide a fertile field for the burgeoning of said right. In fact, our lexicographers have yet to coin a word for it in the Filipino language. Customs and practices, being what they have always been, Filipinos think it perfectly natural and in good taste to inquire into each other's intimate affairs.

One has only to sit through a televised talk show to be convinced that what passes for wholesome entertainment is actually an invasion into one's private life, leaving the interviewee embarrassed and outraged by turns.

With the overarching influence of common law and the recent advent of the Information Age with its high-tech devices, the right to privacy has expanded to embrace its public law aspect. The Bill of Rights of our evolving Charters, a direct transplant from that of the United States, contains in essence facets of the right to privacy which constitute limitations on the far-reaching powers of government.

So terrifying are the possibilities of a law such as Administrative Order No. 308 in making inroads into the private lives of the citizens, a virtual Big Brother looking over our shoulder, that it must, without delay, be "slain upon sight" before our society turns totalitarian with each of us, a mindless robot.

I, therefore, VOTE for the nullification of A.O. No. 308.

VITUG, *J.,* separate opinion;

One can appreciate the concern expressed by my esteemed colleague, Mr. Justice Reynato S. Puno, echoing that of the petitioner, the Honorable Blas F. Ople, on the issuance of Administrative Order No. 308 by the President of the Philippines and the dangers its implementation could bring. I find it hard, nevertheless, to peremptorily assume at this time that the administrative order will be misused and to thereby ignore the possible benefits that can be derived from, or the merits of, a nationwide computerized identification reference system. The great strides and swift advances in technology render it inescapable that one day we will, at all events, have to face up with the reality of seeing extremely sophisticated methods of personal identification and any attempt to stop the inevitable may either be short-lived or even futile. The imperatives, I believe, would instead be to now install specific safeguards and control measures that may be calculated best to ward-off probable ill effects of any such device. Here, it may be apropos to recall the pronouncement of this Court in *People vs. Nazario* [1] that —

> As a rule, a statute or [an] act may be said to be vague when it lacks comprehensible standards that men "of common intelligence must necessarily guess at its meaning and differ as to its application." It is repugnant to the Constitution in two respects: (1) it violates due process for failure to accord persons, especially the parties targeted by it, fair notice of the conduct to avoid; and (2) it leaves law enforcers unbridled discretion in carrying out its provisions and becomes an arbitrary flexing of the Government muscle. [2]

Administrative Order No. 308 appears to be so extensively drawn that could, indeed, allow unbridled options to become available to its implementors beyond the reasonable comfort of the citizens and of residents alike.

Prescinding from the foregoing, and most importantly to this instance, the subject covered by the questioned administrative order can have far-reaching consequences that can tell on all individuals, their liberty and privacy, that, to my mind, should make it indispensable and appropriate to have the matter specifically addressed by the Congress of the Philippines, the policy-making body of our government, to which the task should initially belong and to which the authority to formulate and promulgate that policy is constitutionally lodged.

WHEREFORE, I vote for the nullification of Administrative Order No. 308 for being an undue and impermissible exercise of legislative power by the Executive.

94

PANGANIBAN, *J.,* separate opinion;

I concur only in the result and only on the ground that an executive issuance is not legally sufficient to establish an all-encompassing computerized system of identification in the country. The subject matter contained in AO 308 is beyond the powers of the President to regulate without a legislative enactment.

I reserve judgmeht on the issue of wherher a national ID system is an infringement of the constitutional right to privacy or the freedom of thought until after Congress passes, if ever, a law to this effect. Only then, and upon the filing of a proper petition, may the provisions of the statute be scrutinized by the judiciary to determine their constitutional foundation. Until such time, the issue is premature; and any decision thereon, speculative and academic. [1]

Be that as it may, the scholarly discussions of Justices Romero, Puno, Kapunan and Mendoza on the constitutional right to privacy and freedom of thought may stil become useful guides to our lawmakers, when and if Congress should deliberate on a bill establishing a national identification system.

Let it be noted that this Court, as shown by the voting of the justices, has not definitively ruled on these points. The voting is decisive only on the need for the appropriate legislation, and it is only on this ground that the petition is granted by this Court.

KAPUNAN, *J.,* dissenting opinion;

The pioneering efforts of the executive to adopt a national computerized identification reference system has met fierce opposition. It has spun dark predictions of sinister government ploys to tamper with the citizen's right to privacy and ominous forecasts of a return to authoritarianism. Lost in the uproar, however, is the simple fact that there is nothing in the whole breadth and lenght of Administrative Order No. 308 that suggests a taint constitutional infirmity.

A.O. No. 308 issued by President Fidel V. Ramos on 12 December 1996 reads:

ADMTNISTRATIVE ORDER NO. 308

ADOPTION OF A NATIONAL COMPUTERIZED

IDENTIFICATION REFERENCE SYSTEM

WHEREAS, there is a need to provide Filipino citizens and foreign residents with the facility to conveniently transact business with basic services and social security providers and other government instrumentalities;

WHEREAS, this will require a computerized system to properly and efficiently identify persons seeking basic services and social security and reduce, if not totally eradicate, fraudulent transactions and misrepresentations;

WHEREAS, a concerted and collaborative effort among the various basic services and social security providing agencies and other government instrumentalities is required to achieve such a system;

NOW, THEREFORE, I, FIDEL V. RAMOS, President of the Repubic of the Philippines, by virtue of the powers vested in me by law, do hereby direct the following:

Sec. 1 *Establishment of a National Computerized Identification Reference System.* A decentralized Identification Reference System among the key basic services and social security providers is hereby established.

Sec. 2. *Inter-Agency Coordinating Committee.* An Inter-Agency Coordinating Committee (IACC) to draw-up the implementing guidelines and oversee the implementation of the System is hereby created, chaired by the Executive Secretary, with the following as members:

Head Presidential Management Staff

Secretary, National Economic Development Authority

Secretary, Department of the Interior and Local Government

Secretary, Department of Health

Administrator, Government Service Insurance System

Administrator, Social Security System

Administrator, National Statistics Office

Managing Director, National Computer Center

Sec. 3. *Secretariat.* The National Computer Center (NCC) is hereby designated as secretariat to the IACC and as such shall provide administrative and technical support to the IACC.

Sec. 4. *Linkage Among Agencies.* The Population Reference Number (PRN) generated by the NSO shall serve as the common reference number to establish a linkage among concerned agencies. The IACC Secretariat shall coordinate with the different Social Security and Services Agencies to establish the standards in the use of Biometrics Technology and in computer application designs of their respective systems.

Sec. 5. *Conduct of Information Dissemination Campaign.* The Office of the Press Secretary, in coordination with the National Statistics Offices, the GSIS and SSS as lead agencies and other concerned agencies shall undertake a massive tri-media information dissemination campaign to educate and raise public awareness on the importance and use of the PRN and the Social Security Identification Reference.

Sec. 6. *Funding.* The funds necessary for the implementation of the system shall be sourced from the respective budgets of the concerned agencies.

Sec. 7. *Submission of Regular Reports.* The NSO, GSIS and SSS shall submit regular reports to the Office of the President, through the IACC, on the status of implementation of this undertaking.

Sec. 8 *Effectivity.* This Administartive Order shall take effect immediately.

DONE in the City of Manila, this 12th day of December in the year of Our Lord, Nineteen Hundred and Ninety-Six.

In seeking to strike down A.O. No. 308 as unconstitutional, petitioner argues:

A. THE ESTABLISHMENT OF NATIONAL COMPUTERIZED IDENTIFICATION REFERENCE SYSTEM REQUIRES A LEGISLATIVE ACT. THE ISSUACE OF A.O. NO. 308 BY THE PRESIDENT OF THE REPUBLIC OF THE PHILIPPINES IS, THEREFORE, AN UNCONSTITUTIONAL USURPATION OF THE LEGISLATIVE POWERS OF THE CONGRESS OF THE REPUBLIC OF THE PHILIPPINES.

B. THE APPROPRIATION OF PUBLIC FUNDS BY THE PRESIDENT FOR THE IMPLEMENTATION OF A.O. NO. 308 IS AN UNCONSTITUTIONAL USURPATION OF THE EXCLUSIVE RIGHT OF CONGRESS TO APPROPRIATE PUBLIC FUNDS FOR EXPENDITURE.

C. THE IMPLEMENTATION OF A.O. NO. 308 INSIDIOUSLY LAYS THE GROUNDWORK FOR A SYSTEM WHICH WILL VIOLATE THE BILL OF RIGHTS ENSHRINED IN THE CONSTITUTION.

The National Computerized Identification Reference system to which the NSO, GSIS and SSS are linked as lead members of the IACC is intended to establish uniform standards for ID cards isssued by key government agencies (like the SSS) [1] for the "efficient identification of persons." [2] Under the new system, only one reliable and tamper-proof I.D. need be presented by the cardholder instead of several identification papers such as passports and driver's license, [3] to able to transact with government agencies. The improved ID can be used to facilitate public transactions such as:

1. Payment of SSS and GSIS benefits

2. Applications for driver's license, BIR TIN, passport, marriage license, death certificate, NBI and police clearances, and business permits

3. Availment of Medicare services in hospitals

4. Availment of welfare services

5. Application for work/employment

6. Pre-requisite for Voter's ID. [4]

The card may also be used for private transactions such as:

1. Opening of bank accounts

2. Encashment of checks

3. Applications for loans, credit cards, water, power, telephones, pagers, etc.

4. Purchase of stocks

5. Application for work/employment

6. Insurance claims

7. Receipt of payments, checks, letters, valuables, etc. [5]

The new identification system would tremendously improve and uplift public service in our country to the benefit of Filipino citizens and resident aliens. It would promote, facilitate and speed up legitimate transactions with government offices as well as with private and business entities. Experience tells us of the constant delays and inconveniences the public has to suffer in availing of basic public services and social security benefits because of inefficient and not too reliable means of identification of the beneficiaries.

Thus, in the "Primer on the Social Security Card and Administrative Order No. 308" issued by the SSS, a lead agency in the implementation of the said order, the following salient features are mentioned:

1. A.O. 308 merely establishes the standards for I.D. cards issued by key government agencies such as SSS and GSIS.

2. It does not establish a national I.D. system neither does it require a national I.D. card for every person.

3. The use of the I.D. is voluntary.

4. The I.D. is not required for delivery of any government service. Everyone has the right to basic government services as long as he is qualified under existing laws.

5. The I.D. cannot and will not in any way be used to prevent one to travel.

6. There will be no discrimination Non-holders of the improved I.D. are still entitled to the same services but will be subjected to the usual rigid identification and verification beforehand.

I

The issue that must first be hurdled is: was the issuance of A.O. No. 308 an exercise by the President of legislative power properly belonging to Congress?

It is not.

The Administrative Code of 1987 has unequivocally vested the President with quasi-legislative powers in the form of executive orders, administrative orders, proclamations, memorandum orders and circulars and general or special orders. [6] An administrative order, like the one under which the new identification system is embodied, has its peculiar meaning under the 1987 Administrative Code:

Sec. 3. Administrative Orders. — Acts of the President which relate to particular aspects of governmental operations in pursuance of his duties as administrative head shall be promulgated in administrative orders.

The National Computerized Identification Reference System was established pursuant to the aforaquoted provision precisely because its principal purpose, as expressly stated in the order, is to provide the people with "the facility to conveniently transact business" with the various government agencies providing basic services. Being the "administrative head," it is unquestionably the responsibility of the President to find ways and means to improve the government bureaucracy, and make it more professional, efficient and reliable, specially those government agencies and instrumentalities which provide basic services and which the citizenry constantly transact with, like the Government Service Insurance System (GSIS), Social Security System (SSS) and National Statistics Office (NSO). The national computerized ID system is one such advancement. To emphasize, the new identification reference

system is created to streamline the bureaucracy, cut the red tape and ultimately achieve administrative efficiency. The project, therefore, relates to, is an appropriate subject and falls squarely within the ambit of the Chief Executive's administrative power under which, in order to successfully carry out his administrative duties, he has been granted by law quasi-legislative powers, quoted above.

Understandably, strict adherence to the doctrine of separation of power spawns differences of opinion. For we cannot divide the branches of government into water-tight compartment. Even if such is possible, it is neither desirable nor feasible. Bernard Schwartz, in his work Administrative Law, A Casebook, thus states:

> To be sure, if we think of the separation of powers as carrying out the distinction between legislation and administration with mathematical precision and as dividing the branches of government into watertight compartments, we would probably have to conclude that any exercise of lawmaking authority by an agency is automatically invalid. Such a rigorous application of the constitutional doctrine is neither desirable nor feasible; the only absolute separation that has ever been possible was that in the theoretical writings of a Montesquieu, who looked across at foggy England from his sunny Gascon vineyards and completely misconstrued what he saw. [7]

A mingling of powers among the three branches of government is not a novel concept. This blending of powers has become necessary to properly address the complexities brought about by a rapidly developing society and which the traditional branches of government have difficulty coping with. [8]

It has been said that:

> The true meaning of the general doctrine of the separation of powers seems to be that the whole power of one department should not be exercised by the same hands which possess the whole power of either of the other department, and that no one department ought to possess directly or indirectly an overruling influence over the others. And it has been that this doctrine should be applied only to the powers which because of their nature are assigned by the constitution itself to one of the departments exclusively. Hence, it does not necessarily follow that an entire and complete separation is either desirable of was ever intended, for such a complete separation would be impracticable if not impossible; there may be-and frequently are-areas in which executive, legislative, and judicial powers blend or overlap; and many officers whose duties cannot be exclusively placed under any one of these heads.
>
> The courts have perceived the necessity of avoiding a narrow construction of a state constitutional provision for the division of the powers of the government into three distinct departments, for it is impractical to view the provision from the standpoint of a doctrinaire. Thus, the modern view of separation of powers rejects the metaphysical abstractions and reverts instead to more pragmatic, flexible, functional approach, giving recognition to the fact that then may be a certain degree of blending or admixture of the three powers of the government. Moreover, the doctrine of separation of powers has never been strictly or rigidly applied, and indeed could not be, to all the ramifications of state or national governments; government would prove abortive if it were attempted to follow the policy of separation to the letter. [9]

In any case A.O. No. 308 was promulgated by the President pursuant to the quasi-legislative powers expressly granted to him by law and in accordance with his duty as administrative head. Hence, the contention that the President usurped the legislative prerogatives of Congress has no firm basis.

II

Having resolved that the President has the authority and prerogative to issue A.O. No. 308, I submit that it is premature for the Court to determine the constitutionality or unconstitutionality of the National Computerized Identification Reference System.

Basic in constitutional law is the rule that before the court assumes jurisdiction over and decide constitutional issues, the following requisites must first be satisfied:

1) there must be an actual case or controversy involving a conflict of rights susceptible of judicial determination;

2) the constitutional question must be raised by a proper party;

3) the constitutional question must be raised at the earliest opportunity; and

4) the resolution of the constitutional question must be necessary to the resolution of the case. [10]

In this case, it is evident that the first element is missing. Judicial intervention calls for an actual case or controversy

which is defined as "an existing case or controversy that is appropriate or ripe for determination, *not conjectural or anticipatory*." [11] Justice Isagani A. Cruz further expounds that "(a) justifiable controversy is thus distinguished from a difference or dispute of a hypothetical or abstract character or from one that is academic or moot. The controversy must be definite and concrete, touching the legal relations of parties having adverse legal interests. It must be a real and substantial controversy admitting of special relief through a decree that is conclusive in character, as distinguished from an opinion advising what the law would be upon a hypothetical state of facts. . . ." [12] A.O. No. 308 does not create any concrete or substantial controversy. It provides the general framework of the National Computerized Identification Reference System and lays down the basic standards (efficiency, convenience and prevention of fraudulent transactions) for its cretion. But as manifestly indicated in the subject order, it is the Inter-Agency Coordinating Committee (IACC) which is tasked to research, study and formulate the guidelines and parameters for the use of Biometrics Technology and in computer application designs that will and define give substance to the new system. [13] This petition is, thus, premature considering that the IACC is still in the process of doing the leg work and has yet to codify and formalize the details of the new system.

The majority opines that the petition is ripe for adjudication even without the promulgation of the necessary guidelines in view of the fact that respondents have begun implementation of A.O. No. 308. The SSS, in particular, has started advertising in newspapers the invitation to bid for the production of the I.D. cards. [14]

I beg to disagree. It is not the new system itself that is intended to be implemented in the invitation to bid but only the manufacture of the I.D. cards. Biometrics Technology is not and cannot be used in the I.D. cards as no guidelines therefor have yet been laid down by the IACC. Before the assailed system can be set up, it is imperative that the guidelines be issued first.

III

Without the essential guidelines, the principal contention for invalidating the new identification reference system — that it is an impermissible encroachment on the constitutionally recognized right to privacy — is plainly groundless. There is nothing in A.O. No. 308 to serve as sufficient basis for a conclusion that the new system to be evolved violates the right to privacy. Said order simply provides the system's general framework. Without the concomitant guidelines, which would spell out in detail how this new identification system would work, the perceived violation of the right to privacy amounts to nothing more than mere surmise and speculation.

What has caused much of the hysteria over the National Computerized Identification Reference System is the possible utilization of Biometrics Technology which refers to the use of autnomated matching of physiological or behavioral characteristics to identify a person that would violated the citizen's constitutionally protected right to privacy.

The majority opinion has enumerated various forms and methods of Biometrics Technology which if adopted in the National Computaized Identification Reference System would seriously threaten the right to privacy. Among which are biocrypt retinal scan, artificial nose and thermogram. The majority also points to certain alleged deficiencies of A O. No. 308. Thus:

> 1) A.O. No. 308 does not specify the particular Biometrics Technology that shall be used for the new identification system.
>
> 2) The order dots not state whether encoding of data is limited to biological information alone for identification purposes;
>
> 3) There is no provision as to who shall control and access the data, under what circumstances and for what purpose; and
>
> 4) There are no controls to guard against leakage of information, thus heightening the potential for misuse and abuse.

We should not be overwhelmed by the mere mention of the Biometrics Technology and its alleged, yet unfounded "far-reaching effects."

There is nothing in A.O. No. 308, as it is worded, to suggest that the advanced methods of the Biometrics Technology that may pose danger to the right of privacy will be adopted.

The standards set in A.O. No. 308 for the adoption of the new system are clear-cut and unequivocably spelled out in the "WHEREASES" and body of the order, namely, the need to provide citizens and foreign residents with the facility to *conveniently* transact business with *basic service* and *social security* providers and other government instrumentalities; the computerized system is intended to *properly* and *efficiently* identify persons seeking *basic services or social security* and *reduce, if not totally eradicate fraudulent transactions and misreprentation*; the national identification reference system is established among the *key basic services and social security providers*; and finally, the IACC Secretariat shall coordinate with different Social Security and Services Agencies to establish the *standards* in the use of Biometrics Technology. Consequently, the choice of the particular form and extent of

Biometrics Technology that will be applied and the parameters for its use (as will be defined in the guidelines) will necessarily and logically be guided, limited and circumscribed by the afore-stated standards. The fear entertained by the majority on the potential dangers of this new technology is thus securedly allayed by the specific limitations set by the above-mentioned standards. More than this, the right to privacy is well-esconced in and directly protected by various provisions of the Bill of Rights, the Civil Code, the Revised Penal Code, and certain laws, all so painstakingly and resourcefully catalogued in the majority opinion. Many of these laws provide penalties for their violation in the form of imprisonment, fines, or damages. These laws will serve as powerful deterrents not only in the establishment of any administrative rule that will violate the constitutionally protected right to privacy, but also to would-be transgressors of such right.

Relevant to this case is the ruling of the U.S. Supreme Court in *Whalen v. Roe.* [15] In that case, a New York statute was challenged for requiring physicians to identify patients obtaining prescription drugs of the statute's "Schedule II" category (a class of drugs having a potential for abuse and a recognized medical use) so the names and addresses of the prescription drug patients can be recorded in a centralized computer file maintained by the New York State Department of Health. Some patients regularly receiving prescription for "Schedule II" drugs and doctors who prescribed such drugs brought an action questioning the validity of the statute on the ground that it violated the plaintiffs' constitutionally protected rights of privacy.

In a unanimous decision, the US Supreme Court sustained the validity of the statute on the ground that the patient identification requirement is a reasonable exercise of the State's broad police powers. The Court also held that there is no support in the record for an assumption that the security provisions of the statute will be adiministered improperly. Finally, the Court opined that the remote possibility that judicial supervision of the evidentiary use of particular items of stored information will not provide adequate protection against unwarranted diclosures is not a sufficient reason for invalidating the patient-identification program.

To be sure, there is always a possibility of an unwarranted disclosure of confidential matters enormously accumulated in computerized data banks and in government records relating to taxes, public health, social security benefits, military affairs, and similar matters. But as previously pointed out, we have a sufficient number of laws prohibiting and punishing any such unwarranted disclosures. Anent this matter, the observation in *Whalen vs. Roe* is instructive:

> . . . We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces and the enforcement of the criminal laws all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. . . . [16]

The majority laments that as technology advances, the level of reasonably expected privacy decreases. That may be true. However, court should tread daintily on the field of social and economic experimentation lest they impede or obstruct the march of technology to improve public services just on the basis of an unfounded fear that the experimentation violates one's constitutionally protected rights. In the sobering words of Mr. Justice Brandeis:

> To stay experimentation in things social and economic is a grave responsibility. Denial of the right to experiment may be fraught with serious consequences to the Nation. It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country. This Court has the power to prevent an experiment. We may strike down the statute which embodies it on the ground that, in our opinion, the measure is arbitary, capricious or unreaonable. We have power to do this, because the due process clause has been held by he Court applicable to matters of substantive law as well as to matters of procedure. But in the exercise of this high power, we must be ever on our guard, lest we erect our prejudices into legal principles. If we would guide by the light of reason, we must let our minds be bold. [17]

Again, the concerns of the majority are premature precisely because there are as yet no guidelines that will direct the Court and serve as solid basis for determining the constitutionality of the new identification system. The Court cannot and should not anticipate the constitutional issues and rule on the basis of guesswok. The guidelines would, among others, determine the particular biometrics method that would be used and the specific personal data that would be collected provide the safeguard, (if any) and supply the details on how this new system in supposed to work. The Court should not jump the gun on the Executive.

III

On the issue of funding, the majority submits that Section 6 of A.O. No. 308, which allows the government agencies included in the new system to obtain funding form their respective budgets, is unconstitutional for being an illegal transfer of appropriations.

It is not so. The budget for the national identification system cannot be deemed a transfer of funds since the same is composed of and will be implemented by the member government agancies. Morever, thses agencies particularly the GSIS and SSS have been issuing some form of identification or membership card. The improved ID cards that will be issued under this new system would just take place of the old identification cards and budget-wise, the funds that were being used to manufacture the old ID cards, which are usually accounted for under the "Supplies and Materials" item of the Government Accounting and Auditing Manual, could now be utilized to fund the new cards. Hence, what is envisioned is not transfer of appropriations but a pooling of funds and resources by the various government agencies involved in the project.

WHEREFORE, I vote to dismiss the petition.

MENDOZA, *J.*, separate opinion;

My vote is to dismiss the petition in this case.

First. I cannot find anything in the text of Administrative Order No. 308 of the President of the Philippines that would warrant a declaration that it is violative of the right of privacy. So far as I can see, all the Administrative Orders does is

> • establish an Identification Reference System involving the following service agencies of the government:
>
> ° Presidential Management Staff
>
> ° National Economic Developemnt Authority
>
> ° Department of the Interior and Local Government
>
> ° Department of Health
>
> ° Government Service Isurance System
>
> ° Social Security Office
>
> ° National Computer Center
>
> • create a committee, composed of the heads of the agencies concerned, to draft rules for the System;
>
> • direct the use of the Population Reference Number (PRN) generated by the National Census and Statistics Office as the common reference number to link the participating agencies into an Identification Reference System, and the adoption by the agencies of standards in the use of biometrics technology and computer designs; and
>
> • provide for the funding of the System from the budgets of the agencies concerned.

Petitioner argues, however, that "the implementation of A.O. No. 308 will mean that each and every Filipino and resident will have a file with the government containing, at the very least, his *PRN* and physiological biometrics such as, but not limited to, his facial features, hand geometry, retinal or iris pattern, DNA pattern, fingerprints, voice characteristics, and signature analysis."

In support of his contention, petitioner quotes the following publication surfed from the Internet:

> *The use of biometrics is the means by which an individual may be conclusively identified. There are two types of biometrics identifiers; Physical and behavioral characteristics, Physiological biometrics include facial features, hand geometry, retinal and iris patterns. DNA, and fingerprints characteristics include voice characteristics and signature analysis.* [1]

I do not see how from the bare provisions of the Order, the full text of which is set forth in the majority opinion, petitioner and the majority can conclude that the Identification Reference System establishes such comprehensive personal information dossiers that can destroy individual privacy. So far as the Order provides, all that is contemplated is an identification system based on data which the government agencies involved have already been requiring individuals making use of their services to give.

For example, under C.A. No. 591, §2(a) the National Statistics Office collects "by enumeration, sampling or other methods, statistics and other information concerning population . . . social and economic institutions, and such other

statistics as the President may direct." In addition, it is in charge of the administration of the Civil Register, [2] which means that it keeps records of information concerning the civil status of persons, *i.e.*, (a) births, (b) deaths, (c) marriages and their annulments; (d) legitimations, (e) adoptions, (f) acknowledgments of natural children, (g) naturalizations, and (h) changes of name. [3]

Other statutes giving government agencies the power to require personal information may be cited. R.A. No. 4136, §23 gives the Land Transportation Office the power to require applicants for a driver's license to give information regarding the following: their full names, date of birth, height, weight, sex, color of eyes, blood type, address, and right thumbprint; [4] while R.A. No. 8239, §5 gives the Department of Foreign Affairs the power to require passport applicants to give information concerning their names, place of birth, date of birth, religious affiliation, marital status, and citizenship.

Justice Romero, tracing the origin of privacy to the attempt of the first man and woman to cover their nakedness with fig leaves, bemoans the fact that technology and institutional pressures have threatened our sense of privacy. On the other hand, the majority would have none of the Identification Reference System "to prevent the shrinking of the right to privacy, once regarded as "the most comprehensive of rights and the right most valued by civilized men."" [5] Indeed, techniques such as fingerprinting or electronic photography in banks have become commonplace. As has been observed, the teaching hospital has come to be accepted as offering madical services that compensate for the loss of the isolation of the sickbed; the increased capacity of applied sciences to utilize more and more kinds of data and the cosequent calls for such data have weakened traditional resistance to disclosure. As the area of relevance, political or scientific, expands, there is strong psychological pressure to yield some ground of privacy. [6]

But this is a fact of life to which we must adjust, as long as the intrusion into the domain of privacy is reasonable. In *Morfe v. Mutuc*, [7] this Court dealt the *coup de grace* to claims of latitudinarian scope for the right of privacy by quoting the pungent remark of an acute observer of the social scene, Carmen Guerrero-Nakpil:

> Privacy? What's that? There is no precise word for it in Filipino, and as far as I know any Filipino dialect and there is none because there is no need for it. The concept and practice of privacy are missing from conventional Filipino life. The Filipino believes that privacy is an unnecessary imposition, an eccentricity that is barely pardonable or, at best, an esoteric Western afterthought smacking of legal trickery. [8]

Justice Romero herself says in her separate opinion that the word privacy is not even in the lexicon of Filipinos.

As to whether the right of privacy is "the most valued right," we do well to remember the encomiums paid as well to other constitutional rights. For Professor Zechariah Chafee, "The writ of habeas corpus is "the most important human rights provision in the fundamental law,"" [9] For Justice Cardozo, on the other hand, freedom of expression "is the matrix, the indispensable condition of nearly every other form of freedom." [10]

The point is that care must be taken in assigning values to constitutional rights for the purpose of calibrating them on the judicial scale, especially if this means employing stricter standards of review for regulations alleged to infringe certain rights deemed to be "most valued by civilized men."

Indeed, the majority concedes that "the right of privacy does not bar all incursions into individual privacy . . . [only that such] incursions into the right must be accompanied by proper safeguards and well-defined standards to prevent unconstitutional invasions." [11] In the case of the Identification Reference System, the purpose is to facilitate the transaction of business with service agencies of the government and to prevent fraud and misrepresentation. The personal identification of an individual can facilitate his treatment in any government hospital in case of emergency. On the other hand, the delivery of material assistance, such as free medicines, can be protected from fraud or misrepresentation as the absence of a data base makes it possible for unscrupulous individuals to obtain assistance from more than one government agency.

Second. Thus, the issue in this case is not really whether A.O. No. 308 violates the right of privacy formed by emanations from the several constitutional rights cited by the majority. [12] The question is whether it violates freedom of thought and of conscience guaranteed in the following provisions of our Bill of Rights (Art. III):

> Sec. 4. No law Shall be passed abridging the freedom of speech, of expression, or of the press, or the right of the people peaceably to assemble and petition the government for redress of grievances.
>
> Sec. 5. No law shall be made respecting an establishment of religion, or prohibiting the free exercise thereof. The free exercise enjoyment of religious profession and worship, without discrimination or preference, shall be forever be allowed. No religious test shall be required for the exercise of civil or political rights.

More specifically, the question is whether the establishment of the Identification Reference System will not result in the compilation of massive dossiers on individuals which, beyond their use for identification, can become

instruments of thought control. So far, the next of A.O. No. 308 affords no basis for believing that the data gathered can be used for such sinister purpose. As already stated, nothing that is not already being required by the concerned agencies of those making use of their servides is required by the Order in question. The Order simply organizes service agencies of the government into a System for the purpose of facilitating the identification of persons seeking basic services and social security. Thus, the whereas clauses of A.O. No. 308 state:

> WHEREAS, there is a need to provide Filipino citizens and foreign residents with the facility to conveniently transact business with basic services and social security providers and other government instrumentalities;
>
> WHEREAS, this will require a computerized system to properly and efficiently identify persons seeking basic services and social security, and reduce, if not totally eradicate, fraudulent transactions and misrepresentations;
>
> WHEREAS, a concerted and collaborative effort among the various basic services and social security providing agencies and other government instrumentalities is required to achieve such a system:

The application of biometric technology and the standardization of computer designs can provide service agencies with precise identification of individuals, but what is wrong with that?

Indeed, A.O. No. 308 is no more than a directive to government agencies which the President of the Philippines has issued in his capacity as administrative head. [13] It is not a statute. It confers no right; it imposes no duty; it affords no protection; it creates no office. [14] It is, as its name indicates, a mere administrative order, the prescise nature of which is given in the following excerpt from the decision in the early case of *Olsen & Co. v. Herstein*: [15]

> [It] is nothing more or less than a command from a superior to an inferior. *It creates no relation except between the official who issues it and the official who receives it.* Such orders, whether executive or departmental, have for their object simply the efficient and economical administration of the affairs of the department to which or in which they are issued in accordance with the law governing the subject-matter. They are administrative in their nature and do not pass beyond the limits of the department to which they are directed or in which they are published, and, therefore, create no rights in third persons. *They are based on, and are the product of a relationship in which power is their source and obedience their object.* Disobedience to or deviation from such an order can be punished only by the power which issued it: and, if that power fails to administer the corrective, then the disobedience goes unpunished. *In that relationship no third person or official may intervene, not even the court.* Such orders may be very temporary, they being subject to instant revocation or modification by the power which published them. Their very nature, as determined by the relationship which prodecued them, demonstrates clearly the impossibility of any other person enforcing them except the one who created them. An attempt on the part of the courts to enforce such orders would result not only in confusion but, substantially, in departmental anarchy also. [16]

Third. There is no basis for believing that, beyond the identification of individuals, the System will be used for illegal purposes. Nor are sanctions lacking for the unauthorized use or disclosure of information gathered by the various agencies constituting the System. For example, as the Solicitor General points out. C.A. No. 591. §4 penalizes the unauthorized use or disclosure of data furnished the NSO with a fine of not more than P600.00 or imprisonment for not more than six months or both.

At all events, at this stage, it is premature to pass on the claim that the Identification Reference System can be used for the purpose of compiling massive dossiers on individuals that can be used to curtail basic civil and political rights since, if at all, this can only be provided in the implementing rules and regulations which have yet to be promulgated. We have already stated that A.O. No. 308 is not a statute. Even in the case of statutes, however, where implementing rules are necessary to put them into effect, it has been held that an attack on their constitutionality would be premature. [17] As Edgar in *King Lear* puts it, "Ripeness is all." [18] For, to borrow some more Shakespearean lines,

> The canker galls the infants of the spring
>
> Too oft before their buttons be disclos'd. [19]

That, more than any doctrine of constitutional law I can think of, succinctly expresses the rule on ripeness, prematurity, and hypothetical, speculative, or conjectural claims.

Of special relevance to this case is *Laird v. Tatum*. [20] There, a class suit was brought seeking declaratory and injunctive relief on the claim that a U.S. Army intelligence surveillance of civilian political activity having "a potential for civil disorder" exercised "a present inhibiting effect on [respondents'] full expression and utilization of their First Amendment rights." In holding the case nonjusticiable, the U.S. Supreme Court, in an opinion by Chief Justice Burger. said: [21]

> In recent years this Court has found in a number of cases that constitutional violations may arise from the deterrent or "chilling," effect of governmental regulations that fall short of a direct prohibition against the exercise of First Amendment rights. [Citation of cases omitted] In none of these cases, however, did the chilling effect arise merely from the individual's knowledge that a governmental agency was engaged in certain activities or from the individual's concomitant fear that, armed with the fruits of those activities, the agency might in the future take some *other* and additional action detrimental to that individual. Rather, in each of these cases, the challenged exercise of governmental power was regulatory, proscriptive, or compulsory in nature, and the complainant was either presently or prospectively subject to the regulations, proscriptions, or compulsions that he was challenging. . . .
>
> [T]hese decisions have in no way eroded the "established principle that to entitle a private individual to invoke the judicial power to determine the validity of executive or legislative action he must show that he was sustained or is immediately in danger of sustaining a direct injury as the result of that action. . . .
>
> The respondents do not meet this test; [the] alleged "chilling" effect may perhaps be seen as arising from respondents' perception of the system as inappropriate to the Army's role under our form of government, or as arising from respondents' beliefs that it is inherently dangerous for the military to be concerned with activities in the civilian sector, or as arising from respondents' less generalized yet speculative apprehensiveness that the Army may at some future date misuse the information in some way that would cause direct harm to respondents. Allegations of a subjective "chill" are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm: "the federal courts established pursuant to Article III of the Constitution do not render advisory opinions." *United Public Workers v. Mitchell*, 330 US 75, 89, 91 L Ed 754, 766, 67 S Ct 556 (1947).

Fourth. Given the fact that no right of privacy is involved in this case and that any objection to the identification Reference System on the ground that it violates freedom of thought is premature, speculative, or conjectural pending the issuance of the implementing rules, it is clear that petitioner Blas F. Ople has no cause of action and, therefore, no standing to bring this action. Indeed, although he assails A.O. No. 308 on the ground that it violates the right of privacy, he claims no personal injury suffered as a result of the Order in question. Instead, he says he is bringing this action as taxpayer, Senator, and member of the Government Service Insurance System.

Insofar as petitioner claims an interest as taxpayer, it is sufficient to say that A.O. No. 308 does not involve the exercise of the taxing or spending power of the government.

Insofar as he purports to sue as a member of the GSIS, neither does petitioner have an intertest sufficient to enable him to litigate a constitutional question. Petitioner claims that in providing that the funds necessary for implementing the System shall be taken from the budgets of the concerned agencies. A.O. No. 308 violates Art. VI, §25(5) which. provides:

> No law shall be passed authorizing any transfer of appropriations; however, the President, the President of the Senate, the Speaker of the House of Representatives, the Chief Justice of the Supreme Court, and the heads of Constitutional Commissions may, by law, be authorized to augment any item in the general appropriations law for their respective offices from savings in other items of their respective appropriations.

But, as the Solicitor General states:

> Petitioner's argument is anchored on two erroneous assumptions: one, that all the concerned agencies, including the SSS and the GSIS, receive budgetary support from the national government; and two, that the GAA is the only law whereby public funds are appropriated. Both assumptions are wrong.
>
> The SSS and GSIS do not presently receive budgetary support from the National Government. They have achieved self-supporting status such that the contributions of their members are sufficient to finance their expenses. One would be hard pressed to find in the GAA an appropriation of funds to the SSS and the GSIS.
>
> Furthermore, their respective charters authorize the SSS and the GSIS to disburse their funds (Rep. Act No. 1161 [1954], as amended, Sec. 25; Pres. Decree No. 1146 [1977], as amended, Sec. 29) without the need for a separate appropriation from the Congress.

Nor as Senator can petitioner claim standing since no power of Congress is alleged to have been impaired by the Administrative Order in question. [22] As already stated, in issuing A.O. No. 308, the President did not exercise the legislative power vested by the Constitution in Congress. He acted on the basis of his own powers as administrative head of the government, as distinguished from his capacity as the Executive. Dean Sinco elucidates the crucial distinction thus:

> The Constitution of the Philippines makes the President not only the executive but also the

> administrative head of the government. . . . Executive power refers to the legal and political function of the President involving the exercise of discretion. Administrative power, on the other hand, concerns itself with the work of applying policies and enforcing orders as determined by proper governmental organs. These two functions are often confused by the public: but they are distinct from each other. The President as the executive authority has the duty of supervising the enforcement of laws for the maintenance of general peace and public order. As administrative head, his duty is to see that every government office is managed and maintained properly by the persons in charge of it in accordance with pertinent laws and regulations.
>
> . . . The power of control vested in him by the Constitution makes for a strongly centralized administrative system. It reinforces further his position as the executive of the government, enabling him to comply more effectively with his constitutional duty to enforce the laws. *It enables him to fix a uniform standard of a administrative eficiency and to check the official conduct of his agents.* The decisions of all the officers within his department are subject to his power of revision, either on his own motion or on the appeal of some individual who might deem himself aggrieved by the action of an administrative official. In case of serious dereliction of duty, he may suspend or remove the officials concerned. [23]

For the foregoing reasons, the petition should be DISMISSED.

 # Separate Opinions

ROMERO, *J.,* separate opinion;

What marks offs man from a beast?

Aside from the distinguishing physical characteristics, man is a rational being, one who is endowed with intellect which allows him to apply reasoned judgment to problems at hand; he has the innate spiritual faculty which can tell, not only what is right but, as well, what is moral and ethical. Because of his sensibilities, emotions and feelings, he likewise possesses a sense of shame. In varying degrees as dictated by diverse cultures, he erects a wall between himself and the outside world wherein he can retreat in solitude, protecting himself from prying eyes and ears and their extensions, whether form individuals, or much later, from authoritarian intrusions.

Piercing through the mists of time, we find the original Man and Woman defying the injunction of God by eating of the forbidden fruit in the Garden. And when their eyes were "opened" forthwith "they sewed fig leaves together, and made themselves aprons." [1] Down the corridors of time, we find man fashioning "fig leaves" of sorts or setting up figurative walls, the better to insulate themselves from the rest of humanity.

Such vague stirrings of the desire "to be left alone," considered "anti-social" by some, led to the development of the concept of "privacy," unheard of among beasts. Different branches of science, have made their own studies of this craving of the human spirit — psychological, anthropological sociological and philosophical, with the legal finally giving its imprimatur by elevating it to the status ofa right, specifically a private right.

Initially recognized as an aspect of tort law, it created giant waves in legal circles with the publication in the Harvard Law Review [2] of the trail-blazing article, "The Right to Privacy," by Samuel D. Warren and Louis D. Brandeis.

Whether viewed as a personal or a property right, it found its way in Philippine Constitutions and statutes; this, in spite of the fact that Philippine culture can hardly be said to provide a fertile field for the burgeoning of said right. In fact, our lexicographers have yet to coin a word for it in the Filipino language. Customs and practices, being what they have always been, Filipinos think it perfectly natural and in good taste to inquire into each other's intimate affairs.

One has only to sit through a televised talk show to be convinced that what passes for wholesome entertainment is actually an invasion into one's private life, leaving the interviewee embarrassed and outraged by turns.

With the overarching influence of common law and the recent advent of the Information Age with its high-tech devices, the right to privacy has expanded to embrace its public law aspect. The Bill of Rights of our evolving Charters, a direct transplant from that of the United States, contains in essence facets of the right to privacy which constitute limitations on the far-reaching powers of government.

So terrifying are the possibilities of a law such as Administrative Order No. 308 in making inroads into the private lives of the citizens, a virtual Big Brother looking over our shoulder, that it must, without delay, be "slain upon sight" before our society turns totalitarian with each of us, a mindless robot.

I, therefore, VOTE for the nullification of A.O. No. 308.

VITUG, *J.*, separate opinion;

One can appreciate the concern expressed by my esteemed colleague, Mr. Justice Reynato S. Puno, echoing that of the petitioner, the Honorable Blas F. Ople, on the issuance of Administrative Order No. 308 by the President of the Philippines and the dangers its implementation could bring. I find it hard, nevertheless, to peremptorily assume at this time that the administrative order will be misused and to thereby ignore the possible benefits that can be derived from, or the merits of, a nationwide computerized identification reference system. The great strides and swift advances in technology render it inescapable that one day we will, at all events, have to face up with the reality of seeing extremely sophisticated methods of personal identification and any attempt to stop the inevitable may either be short-lived or even futile. The imperatives, I believe, would instead be to now install specific safeguards and control measures that may be calculated best to ward-off probable ill effects of any such device. Here, it may be apropos to recall the pronouncement of this Court in *People vs. Nazario* [1] that —

> As a rule, a statute or [an] act may be said to be vague when it lacks comprehensible standards that men "of common intelligence must necessarily guess at its meaning and differ as to its application." It is repugnant to the Constitution in two respects: (1) it violates due process for failure to accord persons, especially the parties targeted by it, fair notice of the conduct to avoid; and (2) it leaves law enforcers unbridled discretion in carrying out its provisions and becomes an arbitrary flexing of the Government muscle. [2]

Administrative Order No. 308 appears to be so extensively drawn that could, indeed, allow unbridled options to become available to its implementors beyond the reasonable comfort of the citizens and of residents alike.

Prescinding from the foregoing, and most importantly to this instance, the subject covered by the questioned administrative order can have far-reaching consequences that can tell on all individuals, their liberty and privacy, that, to my mind, should make it indispensable and appropriate to have the matter specifically addressed by the Congress of the Philippines, the policy-making body of our government, to which the task should initially belong and to which the authority to formulate and promulgate that policy is constitutionally lodged.

WHEREFORE, I vote for the nullification of Administrative Order No. 308 for being an undue and impermissible exercise of legislative power by the Executive.

PANGANIBAN, *J.*, separate opinion;

I concur only in the result and only on the ground that an executive issuance is not legally sufficient to establish an all-encompassing computerized system of identification in the country. The subject matter contained in AO 308 is beyond the powers of the President to regulate without a legislative enactment.

I reserve judgmeht on the issue of wherher a national ID system is an infringement of the constitutional right to privacy or the freedom of thought until after Congress passes, if ever, a law to this effect. Only then, and upon the filing of a proper petition, may the provisions of the statute be scrutinized by the judiciary to determine their constitutional foundation. Until such time, the issue is premature; and any decision thereon, speculative and academic. [1]

Be that as it may, the scholarly discussions of Justices Romero, Puno, Kapunan and Mendoza on the constitutional right to privacy and freedom of thought may stil become useful guides to our lawmakers, when and if Congress should deliberate on a bill establishing a national identification system.

Let it be noted that this Court, as shown by the voting of the justices, has not definitively ruled on these points. The voting is decisive only on the need for the appropriate legislation, and it is only on this ground that the petition is granted by this Court.

KAPUNAN, *J.*, dissenting opinion;

The pioneering efforts of the executive to adopt a national computerized identification reference system has met fierce opposition. It has spun dark predictions of sinister government ploys to tamper with the citizen's right to privacy and ominous forecasts of a return to authoritarianism. Lost in the uproar, however, is the simple fact that there is nothing in the whole breadth and lenght of Administrative Order No. 308 that suggests a taint constitutional infirmity.

A.O. No. 308 issued by President Fidel V. Ramos on 12 December 1996 reads:

ADMTNISTRATIVE ORDER NO. 308

ADOPTION OF A NATIONAL COMPUTERIZED

IDENTIFICATION REFERENCE SYSTEM

WHEREAS, there is a need to provide Filipino citizens and foreign residents with the facility to conveniently transact business with basic services and social security providers and other government instrumentalities;

WHEREAS, this will require a computerized system to properly and efficiently identify persons seeking basic services and social security and reduce, if not totally eradicate, fraudulent transactions and misrepresentations;

WHEREAS, a concerted and collaborative effort among the various basic services and social security providing agencies and other government instrumentalities is required to achieve such a system;

NOW, THEREFORE, I, FIDEL V. RAMOS, President of the Repubic of the Philippines, by virtue of the powers vested in me by law, do hereby direct the following:

Sec. 1 *Establishment of a National Computerized Identification Reference System.* A decentralized Identification Reference System among the key basic services and social security providers is hereby established.

Sec. 2. *Inter-Agency Coordinating Committee.* An Inter-Agency Coordinating Committee (IACC) to draw-up the implementing guidelines and oversee the implementation of the System is hereby created, chaired by the Executive Secretary, with the following as members:

Head Presidential Management Staff

Secretary, National Economic Development Authority

Secretary, Department of the Interior and Local Government

Secretary, Department of Health

Administrator, Government Service Insurance System

Administrator, Social Security System

Administrator, National Statistics Office

Managing Director, National Computer Center

Sec. 3. *Secretariat.* The National Computer Center (NCC) is hereby designated as secretariat to the IACC and as such shall provide administrative and technical support to the IACC.

Sec. 4. *Linkage Among Agencies.* The Population Reference Number (PRN) generated by the NSO shall serve as the common reference number to establish a linkage among concerned agencies. The IACC Secretariat shall coordinate with the different Social Security and Services Agencies to establish the standards in the use of Biometrics Technology and in computer application designs of their respective systems.

Sec. 5. *Conduct of Information Dissemination Campaign.* The Office of the Press Secretary, in coordination with the National Statistics Offices, the GSIS and SSS as lead agencies and other concerned agencies shall undertake a massive tri-media information dissemination campaign to educate and raise public awareness on the importance and use of the PRN and the Social Security Identification Reference.

Sec. 6. *Funding.* The funds necessary for the implementation of the system shall be sourced from the respective budgets of the concerned agencies.

Sec. 7. *Submission of Regular Reports.* The NSO, GSIS and SSS shall submit regular reports to the Office of the President, through the IACC, on the status of implementation of this undertaking.

Sec. 8 *Effectivity.* This Administartive Order shall take effect immediately.

DONE in the City of Manila, this 12th day of December in the year of Our Lord, Nineteen Hundred and

Ninety-Six.

In seeking to strike down A.O. No. 308 as unconstitutional, petitioner argues:

> A. THE ESTABLISHMENT OF NATIONAL COMPUTERIZED IDENTIFICATION REFERENCE SYSTEM REQUIRES A LEGISLATIVE ACT. THE ISSUACE OF A.O. NO. 308 BY THE PRESIDENT OF THE REPUBLIC OF THE PHILIPPINES IS, THEREFORE, AN UNCONSTITUTIONAL USURPATION OF THE LEGISLATIVE POWERS OF THE CONGRESS OF THE REPUBLIC OF THE PHILIPPINES.
>
> B. THE APPROPRIATION OF PUBLIC FUNDS BY THE PRESIDENT FOR THE IMPLEMENTATION OF A.O. NO. 308 IS AN UNCONSTITUTIONAL USURPATION OF THE EXCLUSIVE RIGHT OF CONGRESS TO APPROPRIATE PUBLIC FUNDS FOR EXPENDITURE.
>
> C. THE IMPLEMENTATION OF A.O. NO. 308 INSIDIOUSLY LAYS THE GROUNDWORK FOR A SYSTEM WHICH WILL VIOLATE THE BILL OF RIGHTS ENSHRINED IN THE CONSTITUTION.

The National Computerized Identification Reference system to which the NSO, GSIS and SSS are linked as lead members of the IACC is intended to establish uniform standards for ID cards isssued by key government agencies (like the SSS) [1] for the "efficient identification of persons." [2] Under the new system, only one reliable and tamper-proof I.D. need be presented by the cardholder instead of several identification papers such as passports and driver's license, [3] to able to transact with government agencies. The improved ID can be used to facilitate public transactions such as:

1. Payment of SSS and GSIS benefits

2. Applications for driver's license, BIR TIN, passport, marriage license, death certificate, NBI and police clearances, and business permits

3. Availment of Medicare services in hospitals

4. Availment of welfare services

5. Application for work/employment

6. Pre-requisite for Voter's ID. [4]

The card may also be used for private transactions such as:

1. Opening of bank accounts

2. Encashment of checks

3. Applications for loans, credit cards, water, power, telephones, pagers, etc.

4. Purchase of stocks

5. Application for work/employment

6. Insurance claims

7. Receipt of payments, checks, letters, valuables, etc. [5]

The new identification system would tremendously improve and uplift public service in our country to the benefit of Filipino citizens and resident aliens. It would promote, facilitate and speed up legitimate transactions with government offices as well as with private and business entities. Experience tells us of the constant delays and inconveniences the public has to suffer in availing of basic public services and social security benefits because of inefficient and not too reliable means of identification of the beneficiaries.

Thus, in the "Primer on the Social Security Card and Administrative Order No. 308" issued by the SSS, a lead agency in the implementation of the said order, the following salient features are mentioned:

> 1. A.O. 308 merely establishes the standards for I.D. cards issued by key government agencies such as SSS and GSIS.
>
> 2. It does not establish a national I.D. system neither does it require a national I.D. card for every person.
>
> 3. The use of the I.D. is voluntary.

4. The I.D. is not required for delivery of any government service. Everyone has the right to basic government services as long as he is qualified under existing laws.

5. The I.D. cannot and will not in any way be used to prevent one to travel.

6. There will be no discrimination Non-holders of the improved I.D. are still entitled to the same services but will be subjected to the usual rigid identification and verification beforehand.

I

The issue that must first be hurdled is: was the issuance of A.O. No. 308 an exercise by the President of legislative power properly belonging to Congress?

It is not.

The Administrative Code of 1987 has unequivocally vested the President with quasi-legislative powers in the form of executive orders, administrative orders, proclamations, memorandum orders and circulars and general or special orders. [6] An administrative order, like the one under which the new identification system is embodied, has its peculiar meaning under the 1987 Administrative Code:

> Sec. 3. Administrative Orders. — Acts of the President which relate to particular aspects of governmental operations in pursuance of his duties as administrative head shall be promulgated in administrative orders.

The National Computerized Identification Reference System was established pursuant to the aforaquoted provision precisely because its principal purpose, as expressly stated in the order, is to provide the people with "the facility to conveniently transact business" with the various government agencies providing basic services. Being the "administrative head," it is unquestionably the responsibility of the President to find ways and means to improve the government bureaucracy, and make it more professional, efficient and reliable, specially those government agencies and instrumentalities which provide basic services and which the citizenry constantly transact with, like the Government Service Insurance System (GSIS), Social Security System (SSS) and National Statistics Office (NSO). The national computerized ID system is one such advancement. To emphasize, the new identification reference system is created to streamline the bureaucracy, cut the red tape and ultimately achieve administrative efficiency. The project, therefore, relates to, is an appropriate subject and falls squarely within the ambit of the Chief Executive's administrative power under which, in order to successfully carry out his administrative duties, he has been granted by law quasi-legislative powers, quoted above.

Understandably, strict adherence to the doctrine of separation of power spawns differences of opinion. For we cannot divide the branches of government into water-tight compartment. Even if such is possible, it is neither desirable nor feasible. Bernard Schwartz, in his work Administrative Law, A Casebook, thus states:

> To be sure, if we think of the separation of powers as carrying out the distinction between legislation and administration with mathematical precision and as dividing the branches of government into watertight compartments, we would probably have to conclude that any exercise of lawmaking authority by an agency is automatically invalid. Such a rigorous application of the constitutional doctrine is neither desirable nor feasible; the only absolute separation that has ever been possible was that in the theoretical writings of a Montesquieu, who looked across at foggy England from his sunny Gascon vineyards and completely misconstrued what he saw. [7]

A mingling of powers among the three branches of government is not a novel concept. This blending of powers has become necessary to properly address the complexities brought about by a rapidly developing society and which the traditional branches of government have difficulty coping with. [8]

It has been said that:

> The true meaning of the general doctrine of the separation of powers seems to be that the whole power of one department should not be exercised by the same hands which possess the whole power of either of the other department, and that no one department ought to possess directly or indirectly an overruling influence over the others. And it has been that this doctrine should be applied only to the powers which because of their nature are assigned by the constitution itself to one of the departments exclusively. Hence, it does not necessarily follow that an entire and complete separation is either desirable of was ever intended, for such a complete separation would be impracticable if not impossible; there may be-and frequently are-areas in which executive, legislative, and judicial powers blend or overlap; and many officers whose duties cannot be exclusively placed under any one of these heads.

> The courts have perceived the necessity of avoiding a narrow construction of a state constitutional provision for the division of the powers of the government into three distinct departments, for it is impractical to view the provision from the standpoint of a doctrinaire. Thus, the modern view of separation of powers rejects the metaphysical abstractions and reverts instead to more pragmatic, flexible, functional approach, giving recognition to the fact that then may be a certain degree of blending or admixture of the three powers of the government. Moreover, the doctrine of separation of powers has never been strictly or rigidly applied, and indeed could not be, to all the ramifications of state or national governments; government would prove abortive if it were attempted to follow the policy of separation to the letter. [9]

In any case A.O. No. 308 was promulgated by the President pursuant to the quasi-legislative powers expressly granted to him by law and in accordance with his duty as administrative head. Hence, the contention that the President usurped the legislative prerogatives of Congress has no firm basis.

II

Having resolved that the President has the authority and prerogative to issue A.O. No. 308, I submit that it is premature for the Court to determine the constitutionality or unconstitutionality of the National Computerized Identification Reference System.

Basic in constitutional law is the rule that before the court assumes jurisdiction over and decide constitutional issues, the following requisites must first be satisfied:

1) there must be an actual case or controversy involving a conflict of rights susceptible of judicial determination;

2) the constitutional question must be raised by a proper party;

3) the constitutional question must be raised at the earliest opportunity; and

4) the resolution of the constitutional question must be necessary to the resolution of the case. [10]

In this case, it is evident that the first element is missing. Judicial intervention calls for an actual case or controversy which is defined as "an existing case or controversy that is appropriate or ripe for determination, *not conjectural or anticipatory*." [11] Justice Isagani A. Cruz further expounds that "(a) justifiable controversy is thus distinguished from a difference or dispute of a hypothetical or abstract character or from one that is academic or moot. The controversy must be definite and concrete, touching the legal relations of parties having adverse legal interests. It must be a real and substantial controversy admitting of special relief through a decree that is conclusive in character, as distinguished from an opinion advising what the law would be upon a hypothetical state of facts. . . ." [12] A.O. No. 308 does not create any concrete or substantial controversy. It provides the general framework of the National Computerized Identification Reference System and lays down the basic standards (efficiency, convenience and prevention of fraudulent transactions) for its cretion. But as manifestly indicated in the subject order, it is the Inter-Agency Coordinating Committee (IACC) which is tasked to research, study and formulate the guidelines and parameters for the use of Biometrics Technology and in computer application designs that will and define give substance to the new system. [13] This petition is, thus, premature considering that the IACC is still in the process of doing the leg work and has yet to codify and formalize the details of the new system.

The majority opines that the petition is ripe for adjudication even without the promulgation of the necessary guidelines in view of the fact that respondents have begun implementation of A.O. No. 308. The SSS, in particular, has started advertising in newspapers the invitation to bid for the production of the I.D. cards. [14]

I beg to disagree. It is not the new system itself that is intended to be implemented in the invitation to bid but only the manufacture of the I.D. cards. Biometrics Technology is not and cannot be used in the I.D. cards as no guidelines therefor have yet been laid down by the IACC. Before the assailed system can be set up, it is imperative that the guidelines be issued first.

III

Without the essential guidelines, the principal contention for invalidating the new identification reference system — that it is an impermissible encroachment on the constitutionally recognized right to privacy — is plainly groundless. There is nothing in A.O. No. 308 to serve as sufficient basis for a conclusion that the new system to be evolved violates the right to privacy. Said order simply provides the system's general framework. Without the concomitant guidelines, which would spell out in detail how this new identification system would work, the perceived violation of the right to privacy amounts to nothing more than mere surmise and speculation.

What has caused much of the hysteria over the National Computerized Identification Reference System is the possible utilization of Biometrics Technology which refers to the use of autnomated matching of physiological or behavioral characteristics to identify a person that would violated the citizen's constitutionally protected right to

privacy.

The majority opinion has enumerated various forms and methods of Biometrics Technology which if adopted in the National Computaized Identification Reference System would seriously threaten the right to privacy. Among which are biocrypt retinal scan, artificial nose and thermogram. The majority also points to certain alleged deficiencies of A O. No. 308. Thus:

> 1) A.O. No. 308 does not specify the particular Biometrics Technology that shall be used for the new identification system.
>
> 2) The order dots not state whether encoding of data is limited to biological information alone for identification purposes;
>
> 3) There is no provision as to who shall control and access the data, under what circumstances and for what purpose; and
>
> 4) There are no controls to guard against leakage of information, thus heightening the potential for misuse and abuse.

We should not be overwhelmed by the mere mention of the Biometrics Technology and its alleged, yet unfounded "far-reaching effects."

There is nothing in A.O. No. 308, as it is worded, to suggest that the advanced methods of the Biometrics Technology that may pose danger to the right of privacy will be adopted.

The standards set in A.O. No. 308 for the adoption of the new system are clear-cut and unequivocably spelled out in the "WHEREASES" and body of the order, namely, the need to provide citizens and foreign residents with the facility to *conveniently* transact business with *basic service* and *social security* providers and other government instrumentalities; the computerized system is intended to *properly* and *efficiently* identify persons seeking *basic services or social security* and *reduce, if not totally eradicate fraudulent transactions and misreprentation*; the national identification reference system is established among the *key basic services and social security providers*; and finally, the IACC Secretariat shall coordinate with different Social Security and Services Agencies to establish the *standards* in the use of Biometrics Technology. Consequently, the choice of the particular form and extent of Biometrics Technology that will be applied and the parameters for its use (as will be defined in the guidelines) will necessarily and logically be guided, limited and circumscribed by the afore-stated standards. The fear entertained by the majority on the potential dangers of this new technology is thus securedly allayed by the specific limitations set by the above-mentioned standards. More than this, the right to privacy is well-esconced in and directly protected by various provisions of the Bill of Rights, the Civil Code, the Revised Penal Code, and certain laws, all so painstakingly and resourcefully catalogued in the majority opinion. Many of these laws provide penalties for their violation in the form of imprisonment, fines, or damages. These laws will serve as powerful deterrents not only in the establishment of any administrative rule that will violate the constitutionally protected right to privacy, but also to would-be transgressors of such right.

Relevant to this case is the ruling of the U.S. Supreme Court in *Whalen v. Roe*. [15] In that case, a New York statute was challenged for requiring physicians to identify patients obtaining prescription drugs of the statute's "Schedule II" category (a class of drugs having a potential for abuse and a recognized medical use) so the names and addresses of the prescription drug patients can be recorded in a centralized computer file maintained by the New York State Department of Health. Some patients regularly receiving prescription for "Schedule II" drugs and doctors who prescribed such drugs brought an action questioning the validity of the statute on the ground that it violated the plaintiffs' constitutionally protected rights of privacy.

In a unanimous decision, the US Supreme Court sustained the validity of the statute on the ground that the patient identification requirement is a reasonable exercise of the State's broad police powers. The Court also held that there is no support in the record for an assumption that the security provisions of the statute will be adiministered improperly. Finally, the Court opined that the remote possibility that judicial supervision of the evidentiary use of particular items of stored information will not provide adequate protection against unwarranted diclosures is not a sufficient reason for invalidating the patient-identification program.

To be sure, there is always a possibility of an unwarranted disclosure of confidential matters enomously accumulated in computerized data banks and in government records relating to taxes, public health, social security benefits, military affairs, and similar matters. But as previously pointed out, we have a sufficient number of laws prohibiting and punishing any such unwarranted disclosures. Anent this matter, the observation in *Whalen vs. Roe* is instructive:

> . . . We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces and the enforcement of the criminal laws all require the orderly preservation of great

> quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. . . . [16]

The majority laments that as technology advances, the level of reasonably expected privacy decreases. That may be true. However, court should tread daintily on the field of social and economic experimentation lest they impede or obstruct the march of technology to improve public services just on the basis of an unfounded fear that the experimentation violates one's constitutionally protected rights. In the sobering words of Mr. Justice Brandeis:

> To stay experimentation in things social and economic is a grave responsibility. Denial of the right to experiment may be fraught with serious consequences to the Nation. It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country. This Court has the power to prevent an experiment. We may strike down the statute which embodies it on the ground that, in our opinion, the measure is arbitary, capricious or unreaonable. We have power to do this, because the due process clause has been held by he Court applicable to matters of substantive law as well as to matters of procedure. But in the exercise of this high power, we must be ever on our guard, lest we erect our prejudices into legal principles. If we would guide by the light of reason, we must let our minds be bold. [17]

Again, the concerns of the majority are premature precisely because there are as yet no guidelines that will direct the Court and serve as solid basis for determining the constitutionality of the new identification system. The Court cannot and should not anticipate the constitutional issues and rule on the basis of guesswok. The guidelines would, among others, determine the particular biometrics method that would be used and the specific personal data that would be collected provide the safeguard, (if any) and supply the details on how this new system in supposed to work. The Court should not jump the gun on the Executive.

III

On the issue of funding, the majority submits that Section 6 of A.O. No. 308, which allows the government agencies included in the new system to obtain funding form their respective budgets, is unconstitutional for being an illegal transfer of appropriations.

It is not so. The budget for the national identification system cannot be deemed a transfer of funds since the same is composed of and will be implemented by the member government agancies. Morever, thses agencies particularly the GSIS and SSS have been issuing some form of identification or membership card. The improved ID cards that will be issued under this new system would just take place of the old identification cards and budget-wise, the funds that were being used to manufacture the old ID cards, which are usually accounted for under the "Supplies and Materials" item of the Government Accounting and Auditing Manual, could now be utilized to fund the new cards. Hence, what is envisioned is not transfer of appropriations but a pooling of funds and resources by the various government agencies involved in the project.

WHEREFORE, I vote to dismiss the petition.

MENDOZA, *J.*, separate opinion;

My vote is to dismiss the petition in this case.

First. I cannot find anything in the text of Administrative Order No. 308 of the President of the Philippines that would warrant a declaration that it is violative of the right of privacy. So far as I can see, all the Administrative Orders does is

> • establish an Identification Reference System involving the following service agencies of the government:
>
> ° Presidential Management Staff
>
> ° National Economic Developemnt Authority
>
> ° Department of the Interior and Local Government
>
> ° Department of Health
>
> ° Government Service Isurance System

° Social Security Office

° National Computer Center

• create a committee, composed of the heads of the agencies concerned, to draft rules for the System;

• direct the use of the Population Reference Number (PRN) generated by the National Census and Statistics Office as the common reference number to link the participating agencies into an Identification Reference System, and the adoption by the agencies of standards in the use of biometrics technology and computer designs; and

• provide for the funding of the System from the budgets of the agencies concerned.

Petitioner argues, however, that "the implementation of A.O. No. 308 will mean that each and every Filipino and resident will have a file with the government containing, at the very least, his *PRN* and physiological biometrics such as, but not limited to, his facial features, hand geometry, retinal or iris pattern, DNA pattern, fingerprints, voice characteristics, and signature analysis."

In support of his contention, petitioner quotes the following publication surfed from the Internet:

> *The use of biometrics is the means by which an individual may be conclusively identified. There are two types of biometrics identifiers; Physical and behavioral characteristics, Physiological biometrics include facial features, hand geometry, retinal and iris patterns. DNA, and fingerprints characteristics include voice characteristics and signature analysis.* [1]

I do not see how from the bare provisions of the Order, the full text of which is set forth in the majority opinion, petitioner and the majority can conclude that the Identification Reference System establishes such comprehensive personal information dossiers that can destroy individual privacy. So far as the Order provides, all that is contemplated is an identification system based on data which the government agencies involved have already been requiring individuals making use of their services to give.

For example, under C.A. No. 591, §2(a) the National Statistics Office collects "by enumeration, sampling or other methods, statistics and other information concerning population . . . social and economic institutions, and such other statistics as the President may direct." In addition, it is in charge of the administration of the Civil Register, [2] which means that it keeps records of information concerning the civil status of persons, *i.e.*, (a) births, (b) deaths, (c) marriages and their annulments; (d) legitimations, (e) adoptions, (f) acknowledgments of natural children, (g) naturalizations, and (h) changes of name. [3]

Other statutes giving government agencies the power to require personal information may be cited. R.A. No. 4136, §23 gives the Land Transportation Office the power to require applicants for a driver's license to give information regarding the following: their full names, date of birth, height, weight, sex, color of eyes, blood type, address, and right thumbprint; [4] while R.A. No. 8239, §5 gives the Department of Foreign Affairs the power to require passport applicants to give information concerning their names, place of birth, date of birth, religious affiliation, marital status, and citizenship.

Justice Romero, tracing the origin of privacy to the attempt of the first man and woman to cover their nakedness with fig leaves, bemoans the fact that technology and institutional pressures have threatened our sense of privacy. On the other hand, the majority would have none of the Identification Reference System "to prevent the shrinking of the right to privacy, once regarded as "the most comprehensive of rights and the right most valued by civilized men."" [5] Indeed, techniques such as fingerprinting or electronic photography in banks have become commonplace. As has been observed, the teaching hospital has come to be accepted as offering madical services that compensate for the loss of the isolation of the sickbed; the increased capacity of applied sciences to utilize more and more kinds of data and the cosequent calls for such data have weakened traditional resistance to disclosure. As the area of relevance, political or scientific, expands, there is strong psychological pressure to yield some ground of privacy. [6]

But this is a fact of life to which we must adjust, as long as the intrusion into the domain of privacy is reasonable. In *Morfe v. Mutuc*, [7] this Court dealt the *coup de grace* to claims of latitudinarian scope for the right of privacy by quoting the pungent remark of an acute observer of the social scene, Carmen Guerrero-Nakpil:

> Privacy? What's that? There is no precise word for it in Filipino, and as far as I know any Filipino dialect and there is none because there is no need for it. The concept and practice of privacy are missing from conventional Filipino life. The Filipino believes that privacy is an unnecessary imposition, an eccentricity that is barely pardonable or, at best, an esoteric Western afterthought smacking of legal trickery. [8]

Justice Romero herself says in her separate opinion that the word privacy is not even in the lexicon of

Filipinos.

As to whether the right of privacy is "the most valued right," we do well to remember the encomiums paid as well to other constitutional rights. For Professor Zechariah Chafee, "The writ of habeas corpus is "the most important human rights provision in the fundamental law,"" [9] For Justice Cardozo, on the other hand, freedom of expression "is the matrix, the indispensable condition of nearly every other form of freedom." [10]

The point is that care must be taken in assigning values to constitutional rights for the purpose of calibrating them on the judicial scale, especially if this means employing stricter standards of review for regulations alleged to infringe certain rights deemed to be "most valued by civilized men."

Indeed, the majority concedes that "the right of privacy does not bar all incursions into individual privacy . . . [only that such] incursions into the right must be accompanied by proper safeguards and well-defined standards to prevent unconstitutional invasions." [11] In the case of the Identification Reference System, the purpose is to facilitate the transaction of business with service agencies of the government and to prevent fraud and misrepresentation. The personal identification of an individual can facilitate his treatment in any government hospital in case of emergency. On the other hand, the delivery of material assistance, such as free medicines, can be protected from fraud or misrepresentation as the absence of a data base makes it possible for unscrupulous individuals to obtain assistance from more than one government agency.

Second. Thus, the issue in this case is not really whether A.O. No. 308 violates the right of privacy formed by emanations from the several constitutional rights cited by the majority. [12] The question is whether it violates freedom of thought and of conscience guaranteed in the following provisions of our Bill of Rights (Art. III):

> Sec. 4. No law Shall be passed abridging the freedom of speech, of expression, or of the press, or the right of the people peaceably to assemble and petition the government for redress of grievances.
>
> Sec. 5. No law shall be made respecting an establishment of religion, or prohibiting the free exercise thereof. The free exercise enjoyment of religious profession and worship, without discrimination or preference, shall be forever be allowed. No religious test shall be required for the exercise of civil or political rights.

More specifically, the question is whether the establishment of the Identification Reference System will not result in the compilation of massive dossiers on individuals which, beyond their use for identification, can become instruments of thought control. So far, the next of A.O. No. 308 affords no basis for believing that the data gathered can be used for such sinister purpose. As already stated, nothing that is not already being required by the concerned agencies of those making use of their servides is required by the Order in question. The Order simply organizes service agencies of the government into a System for the purpose of facilitating the identification of persons seeking basic services and social security. Thus, the whereas clauses of A.O. No. 308 state:

> WHEREAS, there is a need to provide Filipino citizens and foreign residents with the facility to conveniently transact business with basic services and social security providers and other government instrumentalities;
>
> WHEREAS, this will require a computerized system to properly and efficiently identify persons seeking basic services and social security, and reduce, if not totally eradicate, fraudulent transactions and misrepresentations;
>
> WHEREAS, a concerted and collaborative effort among the various basic services and social security providing agencies and other government instrumentalities is required to achieve such a system:

The application of biometric technology and the standardization of computer designs can provide service agencies with precise identification of individuals, but what is wrong with that?

Indeed, A.O. No. 308 is no more than a directive to government agencies which the President of the Philippines has issued in his capacity as administrative head. [13] It is not a statute. It confers no right; it imposes no duty; it affords no protection; it creates no office. [14] It is, as its name indicates, a mere administrative order, the prescise nature of which is given in the following excerpt from the decision in the early case of *Olsen & Co. v. Herstein*: [15]

> [It] is nothing more or less than a command from a superior to an inferior. *It creates no relation except between the official who issues it and the official who receives it.* Such orders, whether executive or departmental, have for their object simply the efficient and economical administration of the affairs of the department to which or in which they are issued in accordance with the law governing the subject-matter. They are administrative in their nature and do not pass beyond the limits of the department to which they are directed or in which they are published, and, therefore, create no rights in third persons. *They are based on, and are the product of a relationship in which power is their source and obedience their object.* Disobedience to or deviation from such an order can be punished only by the power which

> issued it: and, if that power fails to administer the corrective, then the disobedience goes unpunished. *In that relationship no third person or official may intervene, not even the court.* Such orders may be very temporary, they being subject to instant revocation or modification by the power which published them. Their very nature, as determined by the relationship which prodecued them, demonstrates clearly the impossibility of any other person enforcing them except the one who created them. An attempt on the part of the courts to enforce such orders would result not only in confusion but, substantially, in departmental anarchy also. [16]

Third. There is no basis for believing that, beyond the identification of individuals, the System will be used for illegal purposes. Nor are sanctions lacking for the unauthorized use or disclosure of information gathered by the various agencies constituting the System. For example, as the Solicitor General points out. C.A. No. 591. §4 penalizes the unauthorized use or disclosure of data furnished the NSO with a fine of not more than P600.00 or imprisonment for not more than six months or both.

At all events, at this stage, it is premature to pass on the claim that the Identification Reference System can be used for the purpose of compiling massive dossiers on individuals that can be used to curtail basic civil and political rights since, if at all, this can only be provided in the implementing rules and regulations which have yet to be promulgated. We have already stated that A.O. No. 308 is not a statute. Even in the case of statutes, however, where implementing rules are necessary to put them into effect, it has been held that an attack on their constitutionality would be premature. [17] As Edgar in *King Lear* puts it, "Ripeness is all." [18] For, to borrow some more Shakespearean lines,

> The canker galls the infants of the spring
>
> Too oft before their buttons be disclos'd. [19]

That, more than any doctrine of constitutional law I can think of, succinctly expresses the rule on ripeness, prematurity, and hypothetical, speculative, or conjectural claims.

Of special relevance to this case is *Laird v. Tatum.* [20] There, a class suit was brought seeking declaratory and injunctive relief on the claim that a U.S. Army intelligence surveillance of civilian political activity having "a potential for civil disorder" exercised "a present inhibiting effect on [respondents'] full expression and utilization of their First Amendment rights." In holding the case nonjusticiable, the U.S. Supreme Court, in an opinion by Chief Justice Burger. said: [21]

> In recent years this Court has found in a number of cases that constitutional violations may arise from the deterrent or."chilling," effect of governmental regulations that fall short of a direct prohibition against the exercise of First Amendment rights. [Citation of cases omitted] In none of these cases, however, did the chilling effect arise merely from the individual's knowledge that a governmental agency was engaged in certain activities or from the individual's concomitant fear that, armed with the fruits of those activities, the agency might in the future take some *other* and additional action detrimental to that individual. Rather, in each of these cases, the challenged exercise of governmental power was regulatory, proscriptive, or compulsory in nature, and the complainant was either presently or prospectively subject to the regulations, proscriptions, or compulsions that he was challenging. . . .
>
> [T]hese decisions have in no way eroded the "established principle that to entitle a private individual to invoke the judicial power to determine the validity of executive or legislative action he must show that he was sustained or is immediately in danger of sustaining a direct injury as the result of that action. . .
>
> The respondents do not meet this test; [the] alleged "chilling" effect may perhaps be seen as arising from respondents' perception of the system as inappropriate to the Army's role under our form of government, or as arising from respondents' beliefs that it is inherently dangerous for the military to be concerned with activities in the civilian sector, or as arising from respondents' less generalized yet speculative apprehensiveness that the Army may at some future date misuse the information in some way that would cause direct harm to respondents. Allegations of a subjective "chill" are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm: "the federal courts established pursuant to Article III of the Constitution do not render advisory opinions." *United Public Workers v. Mitchell*, 330 US 75, 89, 91 L Ed 754, 766, 67 S Ct 556 (1947).

Fourth. Given the fact that no right of privacy is involved in this case and that any objection to the identification Reference System on the ground that it violates freedom of thought is premature, speculative, or conjectural pending the issuance of the implementing rules, it is clear that petitioner Blas F. Ople has no cause of action and, therefore, no standing to bring this action. Indeed, although he assails A.O. No. 308 on the ground that it violates the right of privacy, he claims no personal injury suffered as a result of the Order in question. Instead, he says he is bringing this action as taxpayer, Senator, and member of the Government Service Insurance System.

Insofar as petitioner claims an interest as taxpayer, it is sufficient to say that A.O. No. 308 does not involve the

exercise of the taxing or spending power of the government.

Insofar as he purports to sue as a member of the GSIS, neither does petitioner have an intertest sufficient to enable him to litigate a constitutional question. Petitioner claims that in providing that the funds necessary for implementing the System shall be taken from the budgets of the concerned agencies. A.O. No. 308 violates Art. VI, §25(5) which. provides:

> No law shall be passed authorizing any transfer of appropriations; however, the President, the President of the Senate, the Speaker of the House of Representatives, the Chief Justice of the Supreme Court, and the heads of Constitutional Commissions may, by law, be authorized to augment any item in the general appropriations law for their respective offices from savings in other items of their respective appropriations.

But, as the Solicitor General states:

> Petitioner's argument is anchored on two erroneous assumptions: one, that all the concerned agencies, including the SSS and the GSIS, receive budgetary support from the national government; and two, that the GAA is the only law whereby public funds are appropriated. Both assumptions are wrong.
>
> The SSS and GSIS do not presently receive budgetary support from the National Government. They have achieved self-supporting status such that the contributions of their members are sufficient to finance their expenses. One would be hard pressed to find in the GAA an appropriation of funds to the SSS and the GSIS.
>
> Furthermore, their respective charters authorize the SSS and the GSIS to disburse their funds (Rep. Act No. 1161 [1954], as amended, Sec. 25; Pres. Decree No. 1146 [1977], as amended, Sec. 29) without the need for a separate appropriation from the Congress.

Nor as Senator can petitioner claim standing since no power of Congress is alleged to have been impaired by the Administrative Order in question. [22] As already stated, in issuing A.O. No. 308, the President did not exercise the legislative power vested by the Constitution in Congress. He acted on the basis of his own powers as administrative head of the government, as distinguished from his capacity as the Executive. Dean Sinco elucidates the crucial distinction thus:

> The Constitution of the Philippines makes the President not only the executive but also the administrative head of the government. . . . Executive power refers to the legal and political function of the President involving the exercise of discretion. Administrative power, on the other hand, concerns itself with the work of applying policies and enforcing orders as determined by proper governmental organs. These two functions are often confused by the public: but they are distinct from each other. The President as the executive authority has the duty of supervising the enforcement of laws for the maintenance of general peace and public order. As administrative head, his duty is to see that every government office is managed and maintained properly by the persons in charge of it in accordance with pertinent laws and regulations.
>
> . . . The power of control vested in him by the Constitution makes for a strongly centralized administrative system. It reinforces further his position as the executive of the government, enabling him to comply more effectively with his constitutional duty to enforce the laws. *It enables him to fix a uniform standard of a administrative eficiency and to check the official conduct of his agents.* The decisions of all the officers within his department are subject to his power of revision, either on his own motion or on the appeal of some individual who might deem himself aggrieved by the action of an administrative official. In case of serious dereliction of duty, he may suspend or remove the officials concerned. [23]

For the foregoing reasons, the petition should be DISMISSED.

 # Footnotes

1 Dissenting Opinion of Justice Brandeis in Olmstead v. United States, 277 U.S. 438, 478 [1928].

2 Petition, p. 9, *Rollo*, p. 11.

3 Comment, pp. 6, 9, 14, 15, *Rollo*, pp. 65, 68, 73-74.

4 Philconsa vs. Enriquez, 235 SCRA 506 [1994]; Guingona v. PCGG, 207 SCRA 659 [1992]; Tolentino v. Commission on Elections, 41 SCRA 702 [1971].

5 Sanidad v. Commission on Elections, 73 SCRA 333 [1976]; Pascual v. Secretary of Public Works, 110 Phil. 331 [1960].

6 "Invitation to Bid," Annex "E" to the Petition, *Rollo* p. 50.

7 Annex "B" to Petitioner's Reply, *Rollo*, p. 144.

8 Government of the Philippine Islands v. Springer, 50 Phil. 259, 276 [1927].

9 Sec. 1, Article VI, 1987 Constitution.

10 Fernando, The Philippine Constitution, pp. 175-176 [1974].

11 *Id.*, at 177; *citing* the concurring opinion of Justice Laurel in Schneckenburger v. Moran, 63 Phil. 249, 266 [1936].

12 Vera v. Avelino, 77 Phil. 192, 212 [1936].

13 *See* concurring opinion of Justice Laurel in Schneckenburger v. Moran, *supra*, at 266-267.

14 Government of the Philippine Islands v. Springer, 50 Phil. 259, 305 [1927].

15 Sec. 1, Article VII, 1987 Constitution.

16 Cruz, Philippine Political Law, p. 173 [1996].

17 Tanada and Carreon, Political Law of the Philippines, vol. 1, p. 275 [1961].

18 Sec. 17, Article VII of the 1987 Constitution provides:

Sec. 17. The President shall have control of all the executive departments, bureaus and offices. He shall ensure that the laws be faithfully executed.

19 Pelaez v. Auditor General, 15 SCRA 569, 583 [1965].

20 Sinco, Philippine Political Law, pp. 234-235 [1962].

21 *Id.*, at 234.

22 *Id.*, at 235.

23 Sec. 3, Chapter 2, Title I, Book III, Administrative Code of 1987.

24 Cruz, Philippine Administrative Law, p. 18 [1991].

25 Third Whereas Clause, Administrative Code of 1987.

26 Fourth Whereas Clause, Administrative Code of 1987.

27 *See* Cortes, Philippine Administrative Law, pp. 2-5 [1984].

28 Fisher, Constitutional Conflicts Between Congress and the President, 4th ed., pp. 106-107.

29 Cooley on Torts, Sec. 135, vol. 1, 4th ed., [1932]; *see also* Warren and Brandeis "The Right to Privacy," 4 Harvard Law Review 193-220 [1890] — this article greatly influenced the enactment of privacy statutes in the United States (Cortes, I., The Constitutional Foundations of Privacy, p. 15 [1970]).

30 381 U.S. 479, 14 L. ed. 2d 510 [1965].

31 AMENDMENT I [1791]

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

AMENDMENT III [1791]

No Soldier shall, in time of peace be quartered in any house, without the consent of the Owner, nor in time of war, but in a manner to be prescribed by law.

AMENDMENT IV [1791]

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

AMENDMENT V [1791]

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

xxx xxx xxx

AMENDMENT IX [1791]

The enumeration in the Constitutiom, of certain rights, shall not be construed to deny or disparage others retained by the people.

32 22 SCRA 424, 444-445.

33 Morfe v. Mutuc, 22 SCRA 424, 444 [1968]; Cortes, The Constitutional Foundations of Privacy, p. 18 [1970].

34 Cortes, The Constitutional Foundations of Privacy, p. 18 [1970].

35 Art. 26 of the Civil Code provides:

Art. 26. Every person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons. The following and similar acts, though they may not constitute a criminal offense, shall produce a cause of action damages, prevention and other relief:

(1) Prying into the privacy of another's residence;

(2) Meddling with or disturbing the private life or family relations of another;

(3) Intriguing to cause another to be alienated from his friends;

(4) Vexing or humiliating another on account of his religious beliefs, lowly station in life, place of birth, physical defect, or other personal condition.

36 Art. 32, Civil Code.

37 Art. 723, Civil Code.

38 Art. 229, Revised Penal Code.

39 Art. 290-292, Revised Penal Code.

40 Art. 280, Revised Penal Code.

41 R.A. 4200.

42 R.A. 1405.

43 R.A. 8293.

44 Sec. 24, Rule 130 [C], Revised Rules on Evidence.

45 "Biometry," Dorland's Illustated Medical Dictionary, 24th ed. [1965]. "Biometry" or "biometrics" is literally, the measurement of living things; but it is generally used to mean the application of mathematics to biology. The term is now largely obsolete as a biological science since mathematical or statistical work is an integral part of most biological disciplines (The Dictionary of Science [1993]).

46 "Biometric Identification," http://www.afmc.wpafb.af.mil/=organizations/HQ-AFMC/LG/LSO/LOA/bio.html; *see also* "Biometrics Explianed — Section-1,"

http://www.ncsa.com/services/consortia/cbdc/sec1.html.

47 *Id.*

48 *Id.*

49 Or in microchips of smart cards and magnetic strips of bank cards.

50 "Privacy at Risk, Finger-scanning for Ideology and Profit" [1998], file:///D|/commentary.html

51 "Biometric Identification," http://www.afmc.wpafb.af.mil/organizations/HQ-AFMC/LG/LSO/LOA/bio.html

52 "The Libertarian Library: Facing Up to Biometrics," The Mouse Monitor, The International Journal of Bureau-Rat Control [1998], http://www.cyberhaven.com/libertarian/biomet.html.

53 *Id.* The thermogram is so accurate that it can tell identical twins apart and cannot be fooled by cosmetic surgery or disguises, including facial hair.

54 "An updated national population register will provide a suitable base for all types of planning and programming of government facilities and services" (Memorandum of the Solicitor General, p. 20, *Rollo*, p. 210).

55 Similis, "Reviewing Privacy in an Information Society," University of Pennsylvania Law Review, vol. 135: 707, 717 [March 1985].

56 Sloan, I. Law of Privacy Rights in a Technological Society, p. 6 [1986].

57 Respondent GSIS, through counsel claims that the basic information shall be limited to the individual's full name place of birth, date of birth photograph, signature and thumbmark (Comment of Respondent GSIS, p. 6, *Rollo*, p. 101).

58 Olani, K. "Information Security in the Network Age," 70 Philippine Law Journal, 1, 9 [1995].

59 Cortes, I., The Constitutional Foundations of Privacy, p. 12 [1970].

60 Similis, "Reviewing Privacy in an Information Society," University of Pennsylvania Law Review, vol. 135: 707, 740 [March 1987].

61 *Ibid.*, p. 718.

62 The right to control the collection, maintenance use, and dissemination of data about oneself is called "informational privacy" (Hancock, G. "California's Privacy Act: Controlling Government's Use of Information? 32 Stanford Law Review no. 5, p. 1001 [May 1980]. The right to make personal decisions or conduct personal activities without intrusion, observation or interference is called "autonomy privacy" (Hill v. NCAA, 865 p. 2d 633, 652-654 [Cal. 1994].

63 Hosch, "The Interest in Limiting the Disclosure of Personal Information: A Constitutional Analysis," Vanderbilt Law Review vol. 36: 139, 142 [Jan. 1983].

64 Miller, "Personal Privacy in the Computer Age, The Challenge of a New Technology in an Information-Oriented Society," 67 Michigan Law Review 1091, 1119 [1969]; *see also* Cortes, *supra*, at 13.

65 Cortes, I. The Constitutional Foundations of Privacy, p. 12 [1970].

66 *Id.*

67 Rakas v. Illinois, 439 U.S. 128, 143-144 [1978]; *see* the decision and Justice Harlan's concurring opinion in Katz v. United States, 389 U.S. 347, 353, 361, 19 L. ed. 2d 576, 583, 587-589 [1967]; *see also* Southard, "Individual Privacy and Government Efficiency: Techonology's Effect on the Government's Ability to Gather, Store, and Distribute Information" (Computer/Law Journal, vol. IX, pp. 359, 367, note 63 [1989]).

68 Kennedy, "Note: Emasculating a State's Constitutional Right to Privacy: The California Supreme Court's Decision in Hill v. NCAA, "Temple Law Review, vol. 68: 1497, 1517 [1995].

69 *Id.*

70 Southard, *supra*, at 369.

71 *Id*; *see also* Laurence H. Tribe, " The Constitution in Cyberspace: Law and Liberty Beyond the Electronic Frontier," Keynote Address at the First Conference on Computer, Freedom and Privacy, at Jim Warren & Computer Professionals for Social Responsibility [1991].

72 As one author has observed, previously, one could take steps to esure an expectation of privacy in a private palce, e.g., locking of doors and closing of curtains. Because advances in surveillance technology have made these precautions meaningless, the expectation of the privacy they offer is no longer justifiable and reasonable — Southard, *supra*, at 369.

73 Sec. 4, Commenwealth Act No. 591 [1940].

74 Sec. 24 [c] and 28 [e], R.A. 1161, as amended.

75 *Ciling* Morfe v. Mutuc, 22 SCRA 424, 445 [1968].

76 Comment of the Solicitor General, p. 16, *Rollo*, p. 75.

77 Op. cit., note 76.

78 *Id*., at 435.

79 429 U.S. 589, 51 L ed. 2d 64 [1977].

80 Some of the patients were children whose parents feared would be stigmatized by the State's central filing system.

81 Sloan, Law of Privacy Rights in a Technological Society, p. 4 [1986].

82 Southard, "Individual Privacy and Governmental Efficiency: Technology's Effect on the Government's Ability to Gather, Store, and Distribute Information," IX Computer/ Law Journal 359, 360 [1989].

83 The Internet is a decentralized network interconnected by the TCP/IP protocol. The Net was started as a military network ARPANET in 1969 by the US Department of Defense for the purpose of networking main frame computers to prepare against missile weapons. It opened to public research organizations and universities in 1983 and has been interconnected with commercial networks since 1990 (Kazuko Otani, "Information Security in the Network Age," Philippine Law Journal, vol. 70: 1, 2 [1995]).

84 Cyberspace is a place located in no particular geographical location but available to anyone, anywhere in the world, with access to the internet (Darrel Menthe, "Jurisdiction in Cyberspace: A Theory of International Spaces 4 Mich. Tel. Tech. L. Rev. 3 (April 23, 1998), <http://www. law.umich.edu/ mttlr/ volfour/menthe.html>.

85 Southard, *supra*, at 361-362.

86 *Id*; White v. Davis, 533 P. 2d 222 [Cal. 1975]; City of Sta. Barbara v. Adamson, 610 P. 2d 436 [Cal. 1980]. In his concurring opinion in Whalen v. Roe, Justice Brennan stated that a statute that deprives an individual of his privacy is not unconstitutional only if it was necessary to promote a compelling state interest (429 U.S. 589, 606-607, 51 L. ed. 2d 64, 77-78).

87 Morfe v. Mutuc, *supra*, at 444-445 *ciling* Emerson,"Nine Justices in Search of a Doctrine," 64 Michigan Law Review 219, 229 [1965].

88 *See* Shils, "Privacy: Its Constitution and Vicissitudes," Law and Contemporary Problems, vol. 31, pp. 301-303 [1966].

89 Harry Kalvin, Jr., "The Problems of Privacy in the Year 2000," Daedalus, vol. 96, pp. 876-879 [1967].

ROMERO, J., separate opinion;

1 3 Genesis 7.

2 4 Harvard Law Review, 193-220 (1890).

VITUG, J., separate opinion;

1 165 SCRA 186

2 At p. 195.

PANGANIBAN, J., separate opinion;

1 Basic is the doctrine that constitutional issues should not be used to decide a controversy, if there are other available grounds, as in this case. (*See* Justice Isagani Cruz, *Constitutional Law*, 1995 ed., pp. 29-31.)

KAPUNAN, J., dissenting opinion;

1 SSS, Primer on the Social Security Card & A.O. No. 308, p. 1.

2 *Id*, at 2.

3 *Ibid.*

4 *Ibid.*

5 *Id.*, at 3

6 Secs. 2 to 7, Chapter 2, Title I, Book III of the Administrative Code of 1987.

7 Schwartz, Bernard, Administrative Law, a Casebook, Fourth Edition 1994, pp. 78-79.

8 Carlo Cruz Philippines Administrative Law, 1991 ed., pp. 1-3.

9 16 Am Jur. 2d Constitutional Law, Sec. 299. Emphasis supplied.

10 Board of Optometry v. Colet, 260 SCRA 88 (1996).

11 *Ibid.*

12 Isagani A. Cruz, Philippine Political Law, 1991 ed., p. 235.

13 Sec. 2, A.O. No. 308.

14 Annex E, Petition.

15 429 US 589 (1977).

16 *Id.*, at 77.

17 New State Ice Co. v. Liebmann, 285 US 262 (Dissenting Opinion) cited in Whalen v. Roe, 249 US 589.

MENDOZA, J., separate opinion;

1 "Congress Poised To Mandate Government Registration and Tracking of All Americans," *Privacy International*. February 1996; *IDCARD.HTM* at *www.involved.com* (emphasis by petitioner).

2 C.A. No.591, §1(f).

3 Act No. 3753, §1.

4 R.A. No. 4136, §23.

5 Dissenting Opinion of Justice Brandeis in Olmstead v. United States, 438, 478 (1928).

6 Paul A. Freund, Privacy: One Concept or Many, in PRIVACY 188 (R. Pennock and J. Chapman, eds., 1971).

7 22 SCRA 424 (1968).

8 *Id.*, at 445, n. 66.

9 Zechariah Chafee, The Most Important Human Right in the Constitution, 32 BOSTON UNIV. LAW REV. 143 (1947), quoted in Gumabon v. Director of Prisons, 37 SCRA 420, 423 (1971) (per Fernando,

J.).

10 Palko v. Connecticut, 302 U.S. 319, 327, 82 L. Ed. 288, 293 (1937).

11 Majority Opinion, pp. 30-31.

12 The majority *cites* Art. III. §§1, 2, 6, 8, and 1 7 of the Constitution.

13 ADMINISTRATIVE CODE OF 1987, Bk III, Tit I, Ch. I, §3 provides:

Sec. 3. *Administrative Orders.* — Acts of the President which relate to particular aspects of governmental operation in pursuance of his duties as administrative head shall be promulgated in administrative orders.

14 *See* Norton v. Shelby County, 188 U.S. 425, 442, 30 L.Ed 178. 186 (1886).

15 32 Phil. 520 (1915) (emphasis added).

16 *Id.*, at 532.

17 Garcia v. Executive Secretary, 204 SCRA 516 (1991).

18 *King Lear*, Act V, Sc. ii, line 9.

19 Hamlet, Act I, Sc. iii, lines 41-42.

20 408 U.S. 1, 33 L.Ed.2d 154 (1972).

21 *Id.*, 408 U.S. at 13-14, 33 L.Ed.2d at 163-164.

22 Philconsa v. Enriquez, 235 SCRA 506 (1994); Gonzales v. Macaraig, 191 SCRA 452 (1990); Raines v. Byrd, No. 96-1671, June 26, 1997 (Legislators whose votes have been sufficient to defeat (or enact) a specific legislative act have standing to sue if that legislative action goes into effect (or does not go into effect), on the ground that their votes have been completely nullified.")

23 VICENTE G. SINCO, PHILIPPINE POLITICAL LAW 234-235 (11th ed., 1962) (emphasis added).

52

Court of Appeal

*Regina (S) *v* Chief Constable of the South Yorkshire Police

Regina (Marper) *v* Chief Constable of the South Yorkshire Police

[2002] EWCA Civ 1275

2002 July 1, 2; Sept 12

Lord Woolf CJ, Waller and Sedley LJJ

Police — Powers — Retention of evidence — Police taking fingerprints and DNA samples from claimants during course of criminal investigations — Claimants subsequently acquitted or not proceeded against — Police retaining fingerprints and samples — Whether compatible with claimants' right to privacy and not to be discriminated against — Police and Criminal Evidence Act 1984 (c 60), s 64(1A) (as inserted by Criminal Justice and Police Act 2001 (c 16), s 82) — Human Rights Act 1998 (c 42), Sch 1, Pt I, arts 8, 14

The claimant in the first case, a 12-year-old boy, was arrested and charged with attempted robbery and his fingerprints and DNA samples were taken. He was subsequently acquitted. The claimant in the second case was arrested and charged with harassment and his fingerprints and DNA samples were taken. The Crown Prosecution Service subsequently discontinued the case against him. The police wrote to both claimants informing them that under section 64(1A) of the Police and Criminal Evidence Act 1984, as amended[1], the police had the right to retain fingerprints and DNA samples to aid the investigation of crime and that all such fingerprints and samples would be retained. The claimants sought judicial review on the ground that the retention of their fingerprints and samples, when they had not been convicted of a criminal offence, was incompatible with their right to privacy under article 8 and their right not to be discriminated against under article 14 of the Convention for the Protection of Human Rights and Fundamental Freedoms, as scheduled to the Human Rights Act 1998[2]. The Divisional Court dismissed the applications.

On the claimants' appeals—

Held, dismissing the appeals, that the extent to which the retention of fingerprints and samples of DNA was regarded as interfering with the personal integrity of the individual depended very much on the cultural traditions of a particular state; that, in the United Kingdom, fingerprints and DNA samples were material which was regarded as being personal to the individual from whom it was taken and, therefore, the retention of such material by the police under section 64(1A) of the 1984 Act was an interference with an individual's right under article 8(1) to respect for his private life; but that that interference, which although real was not substantial, was justified by, and proportionate to, the need to protect the public from the consequences of crime; that (Sedley LJ dissenting), in considering whether section 64(1A) interfered with an individual's right under article 14 not to be discriminated against, it was necessary to consider the position of all those who had lawfully given fingerprints and samples, and since all those persons were being treated alike section 64(1A) did not involve any interference with the right not to be discriminated against under article 14; that the Chief Constable's policy of normally insisting on retention, but providing for exceptions to be made if exceptional circumstances were shown to

[1] Police and Criminal Evidence Act 1984, s 64, as amended: see post, para 25.
[2] Human Rights Act 1998, Sch 1, Pt I, art 8: see post, para 28.
Art 14: see post, para 29.

53

exist, was a perfectly appropriate policy; and that, accordingly, the police had acted lawfully in retaining the claimants' fingerprints and samples (post, paras 32–34, 39–40, 45–47, 50, 56–59, 63, 65, 67–69).

Per Lord Woolf CJ. If the developments of science expand the purposes for which DNA can be used then the Chief Constable must use his discretion to ensure that the DNA is not used for any purpose not authorised by Parliament. He has ample discretion not to allow samples to be used for purposes contrary to articles 8 and 14 (post, para 54).

Decision of the Divisional Court of the Queen's Bench Division [2002] EWHC 478 (Admin) affirmed.

The following cases are referred to in the judgments:

Aston Cantlow and Wilmcote with Billesley Parochial Church Council v Wallbank [2001] EWCA Civ 713; [2002] Ch 51; [2001] 3 WLR 1323; [2001] 3 All ER 393, CA

Attorney General's Reference (No 3 of 1999) [2001] 2 AC 91; [2001] 2 WLR 56; [2001] 1 All ER 577, HL(E)

Belgian Linguistic Case (No 2) (1968) 1 EHRR 252

British Oxygen Co Ltd v Board of Trade [1971] AC 610; [1970] 3 WLR 488; [1970] 3 All ER 165, HL(E)

Geitling v High Authority of the European Coal and Steel Community (Case 2/56) [1957] ECR 3, ECJ

Griggs v Duke Power Co (1971) 401 US 424

Kinnunen v Finland (Application No 24950/94) (unreported) 15 May 1996, EComHR

McVeigh, O'Neill and Evans v United Kingdom (1981) 5 EHRR 71

R v Weir The Times, 16 June 2000, CA

R (P) v Secretary of State for the Home Department [2001] EWCA Civ 1151; [2001] 1 WLR 2002, CA

Reyntjens v Belgium (1992) 73 DR 136

The following additional cases were cited in argument:

Abdulaziz, Cabales and Balkandali v United Kingdom (1985) 7 EHRR 471

Attorney General of Hong Kong v Lee Kwong-kut [1993] AC 951; [1993] 3 WLR 329; [1993] 3 All ER 939, PC

Botta v Italy (1998) 26 EHRR 241

Brazil v Chief Constable of Surrey [1983] 1 WLR 1155; [1983] 3 All ER 537, DC

Friedl v Austria (1995) 21 EHRR 83

Kjeldsen, Busk Madsen and Pedersen v Denmark (1976) 1 EHRR 711

Lindley v Rutter [1981] QB 128; [1980] 3 WLR 660, DC

Murray v United Kingdom (1994) 19 EHRR 193

R v F (PR) (unreported) 27 December 2001, Court of Appeal for Ontario

R (Samaroo) v Secretary of State for the Home Department [2001] EWCA Civ 1139; The Times, 18 September 2001, CA

Salonen v Finland (Application No 27868/95) (unreported) 2 July 1997, EComHR

Silver v United Kingdom (1983) 5 EHRR 347

Sporrong and Lönnroth v Sweden (1982) 5 EHRR 35

The following additional cases, although not cited, were referred to in the skeleton arguments:

Allenet de Ribemont v France (1995) 20 EHRR 557

Brown v Stott [2001] 2 WLR 817; [2001] 2 All ER 97, PC

de Freitas v Permanent Secretary of Ministry of Agriculture, Fisheries, Lands and Housing [1999] 1 AC 69; [1998] 3 WLR 675, PC

Findlay, In re [1985] AC 318; [1984] 3 WLR 1159; [1984] 3 All ER 801, HL(E)

54

G v Federal Republic of Germany (1989) 60 DR 256
Hilton v United Kingdom (1988) 57 DR 108
Jersild v Denmark (1994) 19 EHRR 1
McMichael v United Kingdom (1995) 20 EHRR 205
R v Arp (1998) 166 DLR (4th) 296
R v Director of Public Prosecutions, Ex p Kebilene [2000] 2 AC 326; [1999] 3 WLR 972; [1999] 4 All ER 801, HL(E)
R (Alconbury Developments Ltd) v Secretary of State for the Environment, Transport and the Regions [2001] UKHL 23; [2001] 2 WLR 1389; [2001] 2 All ER 929, HL(E)
R (Daly) v Secretary of State for the Home Department [2001] UKHL 26; [2001] 2 AC 532; [2001] 2 WLR 1622; [2001] 3 All ER 433, HL(E)
R (Pearson) v Secretary of State for the Home Department [2001] EWHC Admin 239; The Times, 17 April 2001, DC
Rotaru v Romania (Application No 28341/95) (unreported) 4 May 2000, ECHR
S (Minors) (Care Order: Implementation of Care Plan), In re [2002] UKHL 10; [2002] 2 AC 291; [2002] 2 WLR 720; [2002] 2 All ER 192, HL(E)
Sekanina v Austria (1993) 17 EHRR 221
Sunday Times v United Kingdom (1979) 2 EHRR 245

APPEALS from the Divisional Court of the Queen's Bench Division

By an amended claim form filed on 2 January 2002 and with permission granted by Munby J on 19 November 2001 the claimant in the first case, S, applied by his mother and litigation friend, JB, for judicial review of the policy of the defendant, the Chief Constable of the South Yorkshire Police, to retain the fingerprints and samples of all persons who had been investigated in connection with an offence but who, subsequently, were not prosecuted for, or were cleared of, the offence. By a claim form filed on 12 December 2001 and with permission granted by Keith J on 28 January 2002 the claimant in the second case, Michael Raymond Marper, also applied for judicial review of that policy. Both claimants sought an order quashing the policy, and declarations that the Chief Constable had acted in a manner incompatible with their rights under articles 8 and 14 of the Convention for the Protection of Human Rights and Fundamental Freedoms and that section 64 of the Police and Criminal Evidence Act 1984, as amended by section 82 of the Criminal Justice and Police Act 2001, was incompatible with articles 8 and 14 of the Convention to the extent that it permitted the retention of fingerprints and samples of persons with no criminal record. The claimants also sought mandatory orders to enforce the destruction of their fingerprints and samples. On 22 March 2002 the claims were dismissed by the Divisional Court of the Queen's Bench Division (Rose LJ and Leveson J) and permission to appeal was refused.

By notice of appeal filed on 26 April 2001 and with the leave of Laws LJ granted on 28 May 2002 the claimants appealed on the grounds, inter alia, that the Divisional Court had erred in failing to hold (1) that the retention of their fingerprints and samples under section 64 of the 1984 Act, as amended, was incompatible with articles 8 and 14 of the Convention; and (2) that the Chief Constable had fettered his discretion whether to retain fingerprints or samples under section 64.

The facts are stated in the judgment of Lord Woolf CJ.

Richard Gordon QC and *Stephen Cragg* for the claimants.
David Bean QC and *David N Jones* for the Chief Constable.

55

Rabinder Singh QC and *James Strachan* for the Secretary of State for the Home Department as an interested party.

Cur adv vult

12 September. The following judgments were handed down.

LORD WOOLF CJ

Introduction

1 This judgment relates to two appeals. The appeals are against the judgment of the Divisional Court given by Leveson J on 22 March 2002 when sitting with Rose LJ. The point that court decided was that the retention of the fingerprints and DNA samples of individuals who had not been convicted of criminal offences did not contravene either the individual's right to privacy under article 8 or his right not to be discriminated against under article 14 of the Convention for the Protection of Human Rights and Fundamental Freedoms. The Divisional Court therefore dismissed the applications for judicial review made by the claimants, who are respectively a child known as S and Michael Raymond Marper.

2 The two cases provide further examples of the role that courts are now required to perform under the Human Rights Act 1998 of holding the balance between the rights of the individual and the rights of the state. The cases are of particular interest because in this country the public are particularly sensitive about the state unnecessarily retaining personal information about members of the public or requiring members of the public to provide information to the state without good reason. An example of the latter sensitivity being the controversy created by any proposal to require individuals to carry identity cards.

3 On these appeals, it is the retention of fingerprints and DNA samples which were taken during the course of criminal investigations if the prosecutions of the individuals from whom they were taken are either discontinued or result in an acquittal that is challenged. Prior to the coming into force of section 82 of the Criminal Justice and Police Act 2001 on 11 May 2001 the retention of the fingerprints and samples would undoubtedly have been unlawful because of the terms of section 64 of the Police and Criminal Evidence Act 1984 ("PACE"). However, section 64 of PACE was amended by section 82 of the 2001 Act and the section as amended on its literal interpretation undoubtedly authorises their retention in those circumstances.

The facts

4 The appeals are concerned with the issue of principle already identified, but the circumstances of the two cases illustrate admirably how the issue can arise. As the facts are succinctly stated in the judgment of Leveson J I gratefully adopt his account which is in these terms.

The case of S

5 S is a 12-year-old boy. He has no previous convictions, cautions or warnings. On 27 January 2001, following his arrest and being charged with

56

the offence of attempted robbery, his fingerprints and DNA samples were taken. On 14 June 2001, he was acquitted. On 18 July 2001, the principal fingerprint officer of the South Yorkshire Police wrote what appears to be a general letter to the solicitors acting on behalf of S in these terms:

> "I wish to inform you that the South Yorkshire Police will retain fingerprints and samples that were previously required to be destroyed under section 64 of the Police and Criminal Evidence Act 1984. The Criminal Justice and Police Act 2001 now gives the police the right to retain fingerprints and samples to aid crime investigation and is retrospective. All fingerprints and samples that were due for destruction will be retained."

6 It was made clear that the current procedure for the destruction of photographs and negatives had not been altered.

7 Presumably having received that letter, albeit making no reference to it, on 24 July 2001, the solicitors wrote specifically in connection with the case of S and requested that his fingerprints and photographs be destroyed in his presence. Two days later, a letter before action was written to the Chief Constable of the South Yorkshire Police contending that the retention of fingerprints constituted a breach of article 8 of the European Convention on Human Rights and threatening that unless the fingerprints were destroyed, proceedings would be commenced for judicial review seeking a mandatory order for destruction and a declaration of incompatibility.

8 The solicitors wrote a further letter criticising the adoption of a blanket policy on the issue and argued that, even if the legislation was compatible with article 8, the Chief Constable should consider the exercise of his discretion in each case deciding whether retention could be justified by article 8(2); although not specifically mentioned, doubtless at the forefront of the solicitor's mind was the age of S. In connection with that request, evidence filed by the Chief Constable makes it clear that the policy was designed for and does not extend beyond the prevention and detection of crime, the investigation of an offence or the conduct of a prosecution. By way of example of its significance and relevance even to the young, he cites the case of a juvenile, I, whose fingerprints and DNA were taken after his arrest for assault. No prosecution followed and his fingerprints and DNA should have been destroyed; in error they were not. Later both palm print and DNA samples from a rape implicated I. Following the decision in *Attorney General's Reference (No 3 of 1999)* [2001] 2 AC 91, I pleaded guilty to the offence of rape and was sentenced, after appeal, to six years' detention. The Chief Constable makes the point that no reason has been advanced for treating S differently to others in a similar position.

Michael Marper

9 On 13 March 2001, Michael Marper (who was then 38 years of age and is of good character) was arrested and charged with harassment of his partner; his fingerprints and relevant DNA samples were taken that day. He appeared before the court on 23 March 2001 when the case was adjourned to a pre-trial review on 3 May by which time his partner had decided not to press the charge having become reconciled with him. On 11 June, having no doubt accepted that it was no longer in the public interest to force this matter

57

to trial, the Crown Prosecution Service wrote to his solicitors enclosing a notice of discontinuance.

10 On 29 June 2001, Mr Marper's solicitors wrote requesting the destruction of his fingerprints and DNA samples. Having received, dated 18 July 2001, the general letter to which I have already referred, the solicitors wrote again requesting the Chief Constable to exercise his discretion not to retain either fingerprints or samples: the response was to the effect that the position was the same as that set out in the case of S, i e that the Chief Constable had a policy to retain fingerprints and samples in all cases. In these proceedings, the Chief Constable provided an example of a case which he did consider exceptional. In March 2001 W had agreed to be bound over provided, specifically, that her fingerprints, photograph and DNA sample would be destroyed: having regard to the state of the law and policy at that time (which was to destroy this material in those circumstances), that assurance was given. This had not been done by the time the law was changed. When the request was repeated, because of the specific assurance in advance of the bind over, the agreement was honoured and the samples destroyed.

The case for the claimants

11 Mr Gordon on behalf of the claimants advances seven propositions on behalf of the claimants. They are as follows:

(i) The retention of fingerprints and other samples from persons in the position of the claimants constitutes an interference with their right to respect for private life as required by article 8(1) of the Convention ("the article 8(1) issue").

(ii) Such interference is not "in accordance with the law" as article 8(2) requires as the first and most basic prerequisite for justified interference that a measure of this kind (i e section 64 of PACE, as amended) is "in accordance with the law" and for this there must be some identifiable criteria for invoking it and here there are none.

(iii) Further, and in any event, the interference complained of is not necessary in a democratic society for the prevention of crime (or for any other specific aim under article 8(2)) because it is not proportionate to the legitimate aim of preventing crime ((ii) and (iii) together are referred to as "the article 8(2) issue").

(iv) The retention of samples of persons in the claimants' position discriminates, without objective justification, between different groups of members of a relatively similar class, namely between those who have never been suspected of committing a criminal offence and those who have been suspected of or charged with committing a criminal offence but never convicted of a criminal offence. As such the retention is contrary to article 14 of the Convention ("the article 14 issue").

(v) It would be possible to give section 64 of PACE, as amended, "a read down or an implied Convention compatible meaning" to the extent that the court is prepared to read in words excluding from the operation of section 64 the category of persons to whom the claimants belong, namely those who have no previous convictions and who have not been convicted of the offence in respect of which the samples were taken or, at least in respect of such a category of offence, implying into the statute discretionary criteria

58

and procedural safeguards so as to ensure that the retention of samples was proportionate to the legitimate aim of crime prevention.

(vi) To the extent that such a reading cannot be given to the section then section 64 of PACE, as amended, should be declared to be incompatible with articles 8 and 14 of the Convention (together with (v) referred to as "the section 3 of the Human Rights Act 1998 issue").

(vii) Whether or not section 64 of PACE is incompatible with the Convention the policy of the Chief Constable is incompatible with article 8 because: (1) there are no foreseeable criteria for the interference with article 8 and it is, therefore, not in accordance with the law, (2) as expressed it is disproportionate to the (undoubtedly) legitimate aim of preventing crime, (3) it is in breach of article 14 of the Convention, (4) it is (in all but name) a blanket policy and, therefore, in ordinary domestic law a fetter on discretion and (5) it misinterprets the Parliamentary intent in PACE, as amended, because it assumes that Parliament intends no distinction to be drawn between categories of unconvicted persons ("the discretion issue").

12 Both the Secretary of State and the Chief Constable adopted the reasoning of Leveson J for dismissing this appeal. Against the background to the legislation, which he regarded as being of importance, Leveson J came to the conclusion that while the *taking* of fingerprints and DNA samples constituted an interference with a person's private life contrary to article 8(1) he was unclear whether the *retention* of fingerprints and DNA samples was contrary to article 8(1). However, he did not find it necessary to finally determine the position as to *retention* because he was satisfied that the retention was justified by article 8(2). He also came to the conclusion that there was no contravention of article 14. Finally, he decided that the Chief Constable had not unlawfully fettered or otherwise inappropriately exercised his discretion. Rose LJ agreed with the judgment of Leveson J.

13 Prior to the hearing of the appeal, Liberty applied for permission to intervene. Liberty was then given permission to make written submissions. The submissions made by Liberty raised new issues in relation to DNA. As the Secretary of State and the Chief Constable had no opportunity to answer the submissions made by Liberty, they were given a limited period of time to make written submissions in answer to those of Liberty in writing. We will deal with their submissions in the course of dealing with the issues raised by Mr Gordon on behalf of the claimants. The most important feature of Liberty's submissions is that they draw attention to the prospect of DNA samples being used to provide a great deal more information about the persons who provide the samples than is needed for the purposes of the identification of those involved in crime.

14 As is made clear by Mr Gordon's submissions, when resolving this appeal it is necessary to distinguish between the taking, the retention and the use of fingerprints or DNA samples. In the case of DNA it is also necessary to distinguish between DNA samples and the profiles which can be obtained from the samples.

The legislation

15 I turn to the relevant statutory provisions which are contained in PACE, as amended. Leveson J correctly points out that the scheme of the

59

legislation and the history of how it has been amended are important when determining the issues which are raised by this appeal. PACE was intended to play a central role in achieving greater fairness within the criminal justice system and it has undoubtedly made a significant contribution towards achieving that objective. Some of the Act's provisions, a prime example being section 78, assist in fulfilling the purpose of the Act by conferring a broad discretion on the trial judge. Other sections contribute towards achieving the objective by making detailed provisions as to what is to happen in particular circumstances. The sections dealing with the taking, retention and use of fingerprints and samples of DNA fall within this latter category.

16 Whether or not the statutory provisions comply with the articles of the Convention, they undoubtedly represent an attempt by Parliament to achieve a fair balance between the interests of the law-abiding public as a whole and the individual citizen. Where this is the situation, it is important that the courts show appropriate deference to the body whose decision has the advantage of being able to rely on unimpeachable democratic credentials. Any judge, or for that matter any member of the public, will have his or her own opinion as to how the balance should be drawn. However, their individual opinions will lack any democratic support. In considering each of the submissions, of Mr Gordon and Liberty, I regard it as being fundamental that the court keeps at the forefront of its consideration its lack of any democratic credentials.

17 So far as the prevention and detection of crime is concerned, it is obvious the larger the databank of fingerprints and DNA samples available to the police, the greater the value of the databank will be in preventing crime and detecting those responsible for crime. There can be no doubt that if every member of the public was required to provide fingerprints and a DNA sample this would make a dramatic contribution to the prevention and detection of crime. To take but one example, the great majority of rapists who are not known already to their victim would be able to be identified. However, PACE does not contain blanket provisions either as to the taking, the retention, or the use of fingerprints or samples; Parliament has decided upon a balanced approach.

18 The power to retain fingerprints and samples is, of course, subject to such fingerprints and samples having been taken in the first place. The powers and restrictions on the taking of fingerprints and samples are all contained in PACE. Section 27 of PACE, as amended by section 78(1) of the 2001 Act, provides for the taking of fingerprints from a person who has been convicted of a recordable offence, who has not at any time been in police detention for the offence and has not had his fingerprints taken in the course of the investigation of the offence or since the conviction; and the taking of fingerprints from such a person who has had his fingerprints taken before, but the fingerprints taken were not a complete set or were not of sufficient quality to allow statutory analysis, comparison or matching.

19 Section 61(1) of PACE prohibits the taking of any person's fingerprints without the appropriate consent except as provided for by *later subsections of the same* section. Section 61(2) provides that consent for the taking of fingerprints must be in writing if it is given at a time when a person is at a police station. Section 61(3) and (4) provides for the taking of fingerprints without the appropriate consent if a person is detained at a

60

police station, but only where an officer of at least the rank of superintendent (to be replaced by inspector from a day to be appointed under the 2001 Act) authorises them to be taken. Such authorisation may only be given where the officer has reasonable grounds for suspecting the person of a criminal offence, and for believing that his fingerprints will tend to confirm or disprove his involvement (or the fingerprints will facilitate ascertainment of his identity where he has refused to identify himself, or there are reasonable grounds for suspecting he is not who he claims to be—amendment by the Anti-terrorism Crime and Security Act 2001 from a day to be appointed); if the individual has been charged with a recordable offence, or informed he will be reported for such an offence, and he has not had his fingerprints taken in the course of the investigation of that offence by the police: see section 61(3)(b).

20 Section 61(3A) will permit the retaking of fingerprints for persons otherwise falling within section 61(3)(b) if the fingerprints previously taken are not complete, or are not of sufficient quality to allow satisfactory analysis, comparison or matching. This section is added by section 78(3) of the Criminal Justice and Police Act 2001 and is due to come into force on a day to be appointed.

21 Section 61(4A) (as inserted by the 2001 Act) will provide for the taking of fingerprints without the consent of a person who has answered to bail at a court or police station with the consent of the court or an inspector, subject to a requirement of reasonable grounds for believing that the person is not who he claims to be: see section 61(4B).

22 Section 61(6) provides for the taking of fingerprints without consent if the person has been convicted of a recordable offence. This section is amended by section 78(6) of the 2001 Act so that it will apply this power to those given a caution in respect of such an offence, or those who have been warned or reprimanded for such an offence. Section 61(7) imposes a requirement that a person be told of the reason for his fingerprints being taken, and that the reason shall be recorded as soon as practicable. Section 61(7A), as inserted by section 168(2) of and Schedule 10 to the Criminal Justice and Public Order Act 1994, requires that the person shall be informed before the fingerprints are taken, that they may be the subject of a speculative search and the fact that he has been informed of this will be recorded.

23 Similar provisions and restrictions on the taking of intimate samples are provided for under sections 62 and 63 of PACE, subject to additional restrictions on who may take the particular sample. Supplementary powers for the taking of fingerprints and samples, and the checking of fingerprints and samples against other records have been included in section 63A of PACE by section 56 of the 1994 Act, such as the taking of samples in prisons and requiring persons charged with a recordable offence to attend a police station for the taking of a sample.

24 I draw attention to the statutory provisions to which I have referred because they make clear that we are dealing with a situation where Parliament has drawn up a code carefully designed to prescribe the circumstances in which the steps referred to can *and cannot* be taken.

25 Where the provisions of PACE relating to the taking of fingerprints and samples, to which I have referred so far, have been amended by Parliament the general effect of the amendments has been to extend the

61

situations in which the taking of fingerprints and samples is permitted. The same is true of section 64, which deals with their retention. Section 64 of PACE, as amended by section 82 of the 2001 Act, provides, so far as material:

"64. *Destruction of fingerprints and samples.* (1A) Where—(a) fingerprints or samples are taken from a person in connection with the investigation of an offence, and (b) subsection (3) below does not require them to be destroyed, the fingerprints or samples may be retained after they have fulfilled the purposes for which they were taken but shall not be used by any person except for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution . . .

"(3) If—(a) fingerprints or samples are taken from a person in connection with the investigation of an offence; and (b) that person is not suspected of having committed the offence, they must, except as provided in the following provisions of this section be destroyed as soon as they have fulfilled the purpose for which they were taken.

"(3AA) Samples and fingerprints are not required to be destroyed under subsection (3) above if—(a) they were taken for the purposes of the investigation of an offence of which a person has been convicted; and (b) a sample or, as the case may be, fingerprint was also taken from the convicted person for the purposes of that investigation."

26 The most important change introduced by the 2001 Act is that it removes the requirement that if the person from whom the fingerprints or samples were taken in connection with the investigation of an offence is cleared of that offence the fingerprints and samples, subject to specified exceptions, are to be destroyed "as soon as is practicable after the conclusion of the proceedings".

27 Mr Gordon does not suggest that the *taking* of the fingerprints or samples, in accordance with the statutory provisions, contravenes the requirements of articles 8 or 14. He accepts that in that respect the regime contained in PACE, after it has been amended, conforms with the Human Rights Act 1998. His complaint is confined to the fact that their *retention* is authorised after the person from whom they have been taken is no longer being proceeded against as a result of the investigation in connection with which they were taken. In order to understand Mr Gordon's contentions it is necessary to have the language of articles 8 and 14 clearly in mind. The articles are in the following terms:

28 Article 8 provides:

"Right to respect for private and family life

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

"2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

62

29 Article 14 provides:

"Prohibition of discrimination

"The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status."

It is important to note that article 14 does not prohibit all discrimination. It is only concerned with discrimination on grounds "such as" those specified by the article. It is difficult to treat discrimination based on a difference in the treatment between those from whom fingerprints or samples have been lawfully taken from those from whom they have not been taken as falling within the language of the article.

30 When applying articles 8 and 14 of the Convention effect has to be given to sections 2, 3 and 4 of the Human Rights Act 1998. Section 2 requires the court to take into account the decisions of the European Court of Human Rights; section 3 requires the court, so far as it is possible, to interpret legislation in a way which is compatible with the Convention and section 4 requires the court, provided it is satisfied that legislation is incompatible, to consider making a declaration to that effect.

The article 8(1) issue

31 There is no binding authority as to whether the retention of fingerprints and samples of DNA interferes with the right of privacy of the person from whom they are taken. It is conceded that the taking of the fingerprints and samples would do so and that their use probably does so. However, Mr Bean, on behalf of the Chief Constable, and Mr Rabinder Singh contend that Leveson J was right to have doubts on the subject. They argue that there is an important distinction between taking and retention and rely on decisions of the Commission, which they submit are in their favour: see *McVeigh, O'Neill and Evans v United Kingdom* (1981) 5 EHRR 71 and *Kinnunnen v Finland* (Application No 24950/94) (unreported) 15 May 1996. They also seek to distinguish the decisions of the Commission which were relied on by Mr Gordon.

32 The extent to which the retention of material of this nature is regarded as interfering with the personal integrity of the individual, as it seems to me, depends very much on the cultural traditions of a particular state. So far as this jurisdiction is concerned it is my view that fingerprints and DNA samples are material which is regarded as being personal to the individual from whom it is taken and so requires legal justification before it can be retained. This was made clear by the approach of section 64 of PACE before it was amended and is still reflected in the language of the section as amended. I find support in my approach in the speech of Lord Steyn in *Attorney General's Reference (No 3 of 1999)* [2001] 2 AC 91. It would not have been necessary for Lord Steyn to justify the retention under article 8 if the retention being considered in that case was not regarded as being prima facie contrary to article 8(1).

63

33 While I am satisfied that article 8(1) applies to the retention, the extent of the interference with that article is important when considering the next issue, namely whether the interference can be justified under article 8(2). As to this I do not regard the interference as being significant. Here I recognise the relevance of two passages from Leveson J's judgment upon which the Chief Constable and the Secretary of State rely:

> "6. . . . It is important to appreciate that the DNA database is not a list of suspects; rather, it will show only a 'hit' of the DNA profile of an individual which matches that from DNA recovered at a crime scene. Given that DNA can be detected from very small samples (such as might be found on the saliva on a cigarette end) the power of the technique both to eliminate those who might have been suspected or incriminate others is enormous . . .
>
> "19. . . . A person can only be identified by fingerprint or DNA sample either by an expert or with the use of sophisticated equipment or both; in both cases, it is essential to have some sample with which to compare the retained data. Further, in the context of the storage of this type of information within records retained by the police, the material stored says nothing about the physical make-up, characteristics or life of the person to whom they belong."

34 None the less, while not substantial, the interference is still real. There are no doubt a rainbow of reactions which are possible to intrusions of this nature, but at least for a substantial proportion of the public there is a strong objection to the state storing information relating to an individual unless there is some objective justification for this happening. The objection to the storage is reflected in the appreciative public response to novels such as Aldous Huxley's *Brave New World* and George Orwell's *1984*. As to the persuasive decisions of the Commission, it has to be remembered that just as in the appropriate circumstances a margin of appreciation has to be extended for any shortcomings in this jurisdiction in relation to observing the Convention, so there can be situations where the standards of respect for the rights of the individual in this jurisdiction are higher than those required by the Convention. There is nothing in the Convention setting a ceiling on the level of respect which a jurisdiction is entitled to extend to personal rights. In this jurisdiction I would not expect a court to necessarily follow the decision of the Commission in *Reyntjens v Belgium* (1992) 73 DR 136, 152 that: "The obligation to carry an identity card and to show it to the police whenever requested to do so does not as such constitute an interference in a person's private life within the meaning of article 8 of the Convention."

35 It is also to be noted in relation to the last remarks of Leveson J cited that the information relating to the genetic make up of an individual which can be obtained from a DNA sample is continually expanding.

The article 8(2) issue

36 Having surmounted the first hurdle as to whether article 8(1) applies, Mr Gordon argues that no sufficient justification for the retention has been advanced by either the Secretary of State or the Chief Constable. The catalyst for the amendment to section 64 introduced by the 2001 Act were two prosecutions in which the prosecution had relied on DNA samples

64

A which should have been destroyed. In *R v Weir* The Times, 16 June 2000 a conviction of murder was quashed because of the evidence obtained from a DNA sample which had been unlawfully retained being given at the trial. In the other case *R v B* the judge refused to allow the evidence to be given and this resulted in the decision of the House of Lords to which reference has already been made, *Attorney General's Reference (No 3 of 1999)* [2001] 2 AC 91. In that case it was decided that the fact that the sample had been kept in contravention of the then provisions of PACE did not mean that the evidence necessarily had to be excluded. Instead it was a question for the judge under section 78 of PACE. Lord Steyn expressed his approach which was to be adopted in these terms, at p 118:

B

> "It must be borne in mind that respect for the privacy of defendants is not the only value at stake. The purpose of the criminal law is to permit everyone to go about their daily lives without fear of harm to person or property. And it is in the interests of everyone that serious crime should be effectively investigated and prosecuted. There must be fairness to all sides. In a criminal case this requires the court to consider a triangulation of interests. It involves taking into account the position of the accused, the victim and his or her family, and the public."

C

D

Then in answer to the argument that use of a sample, which should have been destroyed, itself constituted a breach of article 8, he added, at p 119:

> "Counsel submitted that, because a sample must be destroyed after an acquittal, it cannot ever be 'in accordance with the law' to admit in evidence the results of a prohibited investigation. The question whether it meets this requirement is the very issue of interpretation which the House has to decide. If the construction I have adopted is correct 'the interference' is 'in accordance with law', the critical point being that admissibility is governed by judicial discretion under section 78. And 'the interference', so qualified, is plainly necessary in a democratic society to ensure the investigation and prosecution of serious crime. There is plainly no breach of article 8."

E

F

37 Lord Steyn was clearly of the opinion that in its unamended form section 64 did not attach sufficient significance to the importance of protecting the public against the consequences of crime. In the House of Commons, on 29 January 2001 (Hansard (HC Debates), cols 42–43), the Home Secretary when supporting the proposed amendment referred to Lord Steyn's speech and said:

G

> "DNA profiling is a very powerful tool—an objective form of evidence. Its value lies as much, if not more, in its ability to exclude the innocent as in its ability to convict the guilty. When the police investigate a case, if they do not proceed with a prosecution or the suspect is acquitted, they routinely retain all the records of the investigation, including the notes of interviews with suspects and other interviews. That has always been the case. The police would not dream of throwing away their memory on the off chance that the offender may or may not commit a further offence. Yet the law requires that the most objective and powerful forms of evidence—fingerprints and DNA—have to be destroyed if a conviction does not follow from the taking of the sample in question. This has already led to

H

65

serious miscarriages of justice. In two recent cases, *R v B* and *R v Weir*, compelling DNA evidence that linked one suspect to a rape and the other to a murder could not be used, and neither suspect could be convicted, because it turned out that at the time when the matches were made, the defendants had either been acquitted of another crime, or a decision had been made not to proceed with the offences for which the DNA profiles were originally taken. Under the existing provisions, the profiles should have been destroyed. Those who believe that we should leave the law as it is, following the decision of the Law Lords in the case of *R v B*, should, I suggest, look at the narrative of Lord Steyn in that case. Their Lordships sought to bring the law as near as possible to common sense without actually murdering the text of the statute, but they could not go the whole way. Lord Steyn pointed out that there were added injustices in the *R v B* case. First, it was unjust to the victim and the community that compelling evidence against this man could not be used to convict him when everyone knew it existed. Secondly, the man was able to escape that conviction altogether only because of another trick—another offence—that he had played on the police. It turned out subsequently that, at the time of his arrest on this charge, he had already been convicted of affray. Had the DNA technology been available and in use when he was arrested on that affray charge and subsequently convicted, it would have been perfectly lawful to take a DNA sample from him and for that to remain on the record for ever. However, the sample was not taken . . . I accept that the use of DNA and fingerprinting must be carefully controlled, precisely because they are powerful tools. However, anyone who has visited a forensic service science laboratory, as I have, and seen the huge care that is taken, will know that it is virtually impossible for any scientist to know whether a sample is to be used to identify a suspect or a victim, and will appreciate the substantial safeguards that are in place. Furthermore, an important role is played by defence counsel in challenging the integrity of the lifting of samples at a scene of crime—by definition, a less controlled environment—and such issues sometimes have to be challenged by the courts. Taking all those arguments together, I believe that the current state of the law is wholly unsatisfactory."

38 The Chief Constable and the Secretary of State strongly rely on the extent of the parliamentary scrutiny of the 2001 Act. It was extensive both in the House of Commons and in the House of Lords. In addition the Joint Committee on Human Rights carefully considered whether the amendment to section 64 met the requirements of article 8(2). The Joint Committee's Report issued on 23 April 2001 (HL Paper 69, HC 427) deals with the amended section 64 provisions at paragraphs 86–92. In that report, the Joint Committee stated, at paragraph 88, that:

"When we first looked at the Bill, we took the view that the clauses [in relation to the retention of fingerprints and samples] amounted to an interference with the person's right to respect for private life (article 8(1) of the Convention), but that they provided a sound legal basis for retention, by ensuring that the circumstances in which retention and use were to be permitted were sufficiently clearly defined, appropriately directed, and limited in scope, in order to satisfy the justifying conditions under article 8(2)."

66

39 Mr Gordon strongly contests the correctness of the Joint Committee's assessment of the amendment but I respectfully agree with the Committee's approach. I regret to say that I cannot understand Mr Gordon's submission that no justification has been shown for the amendment. Its purpose is obvious. The purpose is lawful. It is strictly confined to situations in which fingerprints and samples have been taken in accordance with article 8. The fingerprints and samples can only be used for a purpose of "the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution". Language which is very similar to that in article 8(2).

40 In addition I regard the retention as being proportionate. By confining the retention to fingerprints and samples which have already lawfully been taken the amended provision limits the article 8(1) interference significantly. As against that limited intrusion the scale of the database and therefore its value is substantially increased. I find myself in complete agreement with the Divisional Court that the interference with article 8(1) rights of the individuals from whom the fingerprints and samples are taken is justified by article 8(2)

41 In considering whether the interference with article 8(1) is justified, it is relevant that if my approach to the article is correct, in this jurisdiction article 8(1) may have a longer reach than is strictly required by the Convention as applied by Strasbourg. If this is the result of the approach of society here then Parliament, as the democratically elected body representative of the public, has undoubtedly the untrammelled right to establish the circumstances in which interference is justified as long as it does not fall below the standard set by the Convention, proportionality.

42 Mr Gordon placed great stress on the principle of proportionality but in this situation where the court is required to balance the interests of the individual as against those of the public, the balancing act itself will usually absorb any issue as to proportionality. Sometimes in relation to proportionality a distinction is drawn between a balancing test and a necessity test. The necessity test meaning that if a particular objective can be attained by more than one available means, the least harmful must be adopted (see e g *Clayton & Tomlinson, The Law of Human Rights* (2000), paras 6.57–6.59). However, here there were not alternative ways in which the same benefits could be obtained for the public. If there had been then in considering where the balance of advantage lay the alternative methods of achieving the same or a similar benefit for the public would have to be taken into account. Here the question is, are the adverse consequences to the individual out of proportion to the benefit of the public?; if so, there is no defence under article 8(2). But in my judgment they are not.

The article 14 issue

43 There remains a further hurdle, which the amendment to section 64 must overcome. The amendment must not be discriminatory "on any ground" *specified in article 14*. The amendment applies to those once suspected of crime that, because they are no longer being proceeded against and have not been convicted, are entitled to be regarded as innocent. In this jurisdiction there cannot be different categories of innocence. The non-proven status is not part of English law.

67

44 Mr Gordon therefore contends that the category of persons who were being investigated for a crime but are no longer the subject of proceedings are being discriminated against when their position is compared with that of members of the public who have not been investigated. Mr Gordon submits, and I accept his submission, that both categories are entitled to be regarded as innocent. He therefore contends it would not be right for the court to draw a distinction between one category of innocent person and another. Any member of the public is entitled to be regarded as innocent until the contrary is proved.

45 However, the presumption of innocence does not provide an immunity against being investigated in relation to a criminal offence or against criminal proceedings and the fingerprints and samples were lawfully taken in conjunction with a bona fide investigation. Once the fingerprints and samples are lawfully obtained there is a perfectly clear objective distinction between individuals from whom fingerprints or samples have been taken and those individuals from whom they have not been taken. Without there being any improper discrimination it is proper to treat those who have already given fingerprints or samples differently from those who have not when it comes to the question of the retention of fingerprints or samples. I emphasise that it is this distinction which justifies the different treatment. It would be highly undesirable for members of the public to be treated differently on the basis of some scale of innocence devised by the police.

46 In the present circumstances when an offence is being investigated or is the subject of a charge it is accepted that fingerprints and samples may be taken. Where they have not been taken before any question of the retention arises they have to be taken so there would be the additional interference with their rights which the taking involves. As no harmful consequences will flow from the retention unless the fingerprints or sample match those of someone alleged to be responsible for an offence the different treatment is fully justified.

47 There is also the question of whether the discrimination relied upon is within the categories of discrimination referred to in article 14. It is wholly different from the categories specifically mentioned in the article and I do not consider that it does. It would be highly undesirable if it did. If it did contravene article 14 the result could be that so as to avoid discrimination the categories from whom fingerprints and samples can be taken and retained would be expanded so far as is necessary to avoid discrimination. An approach which could have this effect instead of increasing the protection of human rights could result in that protection being reduced, if, as could well be the case, a universal requirement to provide fingerprints and samples could not be justified. In my opinion section 64, as amended, does not contravene article 14.

48 I do not propose to deal with the Commonwealth authorities relied upon by Mr Gordon because like the Divisional Court I do not regard them as being of assistance. The legislation, which was being considered in those cases, is in different terms. In addition this is an area where under the Human Rights Act 1998 the courts are required to exercise considerable deference to Parliament. This does not mean that this court has not to form its own judgment of the issues, which are raised. It does mean we should not intervene without fully taking into account that the issues are of a category

68

in relation to which Parliament should be recognised as having a special responsibility. A responsibility with which a court should not interfere without clear cause.

The fourth and fifth issues

49 In view of the conclusions to which I have already come these issues do not arise for consideration. There remains only for consideration the allegation that the Chief Constable has wrongly exercised his discretion to which I now turn.

The discretion issue

50 Section 64, as amended, does not require the Chief Constable to retain any fingerprints or samples, which have been taken. He "may" do so. However, as is the case with any other statutory discretion this discretion has to be exercised to further the purpose for which it was conferred. Here that purpose is the prevention and detection of crime. Without casting any reflection on the individuals from whom the fingerprints or samples have been taken who are not still the subject of investigation or have been acquitted the statutory purpose will normally favour retention of the fingerprints or samples unless there are special circumstances justifying the Chief Constable making an exception.

51 Although the Chief Constable failed to make this clear initially, his policy of normally insisting on retention does provide for exceptions to be made, if in any particular case exceptional circumstances are shown to exist. This appears to be a perfectly appropriate policy. It is in accord with the well known approach in *British Oxygen Co Ltd v Board of Trade* [1971] AC 610. I agree with Mr Bean's submission on behalf of the Chief Constable that the comments of Lord Phillips of Worth Matravers MR in *R (P) v Secretary of State for the Home Department* [2001] 1 WLR 2002 do not affect the conclusions set out above.

52 In his judgment, Sedley LJ suggests that the Chief Constable be required to distinguish between different categories of individuals from whom fingerprints or samples have been taken. I do not accept that this is the position. I consider that it would be highly undesirable and inappropriate for Chief Constables to act upon any such distinction.

53 The arguments raised by Liberty have been carefully considered in the judgment of Waller LJ and I entirely agree with the views he has expressed. I accept that the information which can be derived from a sample of DNA is growing rapidly. So are the purposes for which the information can be used. Information may already and certainly in the future will be capable of being obtained from samples which goes well beyond the prevention and detection of crime as now understood. However, the Chief Constable is not contemplating using samples for purposes other than the prevention and detection of crime in the narrow sense, that is in exactly the same way as fingerprints can be used, for identifying or excluding an individual from responsibility for a crime. In its consideration of a case the European Court of Human Rights is careful to confine its judgment to the facts of the case which is before it and, in my judgment, we should adopt the same course and not try to anticipate events.

69

54 The police can make mistakes and act unlawfully but it does not seem to me that the risk that this could happen can affect the outcome of this appeal. The court must assume that the police will act lawfully until the contrary is shown. If the developments of science expand the purposes for which DNA can be used then the Chief Constable must use his discretion to ensure that the DNA is not used for any purpose not authorised by Parliament. He has ample discretion not to allow samples to be used for purposes contrary to article 8 and article 14. There is no need to read the statutory provisions in a restricted manner. If in the future a question arises as to the lawfulness of the use of samples *in a manner that is not now contemplated* that will have to be dealt with when the problem arises.

55 As indicated at the outset of this judgment there is a difference between the DNA profile and the sample. The retention of the sample as well as the profile can be justified by the need to verify the accuracy of the profile. The retention is also appropriate because the developments in relation to DNA may result in the sample being able to be used more effectively for the prevention and detection of crime (in the sense I have indicated) in the future than is possible today.

56 I would dismiss this appeal.

WALLER LJ

57 I agree that the appeal should be dismissed for the reasons given by Lord Woolf CJ. I do not disagree with the views expressed by Sedley LJ save in one important area. I only wish to add some limited comments of my own.

58 It is the submissions of Liberty which have given me most cause for concern. Their submissions convince me that there is a breach of article 8(1) in the retention and use of samples independent from the original breach of that article in the taking of the samples in the first place. Furthermore as I understand their submissions they more readily understand the argument that justification is supplied by article 8(2) if the use to which the samples or DNA profile is put is simply to provide a register or databank against which some other DNA profile can be checked in the future during the investigation of some other offence. If that is the limit of the use of the same *retention* does not actually prejudice the individual from whom the sample has been taken at all, and its use will either clear the person of any suspicion of committing a crime (i e be a benefit to the individual); or provide clear evidence of criminal conduct. The public interest in the prevention of crime must outweigh such infringement as there is of the private interest at this stage just as the taking of samples during a criminal investigation is itself justified. Indeed I would suggest that what Lord Steyn said in *Attorney General's Reference (No 3 of 1999)* [2001] 2 AC 91 quoted by Lord Woolf CJ at paragraph 36 makes the contrary submission impossible. If use of a sample illegally held when permitted in evidence pursuant to the exercise of discretion under section 78 is "plainly no breach of article 8", how can it be a breach to allow the police to retain a sample lawfully if the use is for the "investigation and prosecution of serious crime"?

59 Prior to the passing of section 82 of the 2001 Act, the law was in an unsatisfactory state. Parliament had decreed that lawfully taken samples should be destroyed if persons were acquitted. Yet if such samples were unlawfully retained they could provide cogent evidence relating to the

70

commission of serious crimes. Should Parliament recognise in the public interest that lawfully taken samples should be allowed to be preserved, or should Parliament make unlawfully retained evidence inadmissible with the result that perpetrators of serious offences went free? A full debate took place in Parliament and detailed consideration was given to the Convention. I am fully persuaded that article 8(2) justified the rationalisation of the law.

60 Liberty's concern is that the words "*purposes related to the prevention or detection of crime*" give a very wide discretion. They suggest that this would include intelligence gathering and other forms of collation of detailed personal information, outside the immediate context of the investigation of a particular offence. They recognise that fingerprints and DNA *profiles* reveal only limited personal information. The physical samples potentially contain very much greater and more personal and detailed information. The anxiety is that science may one day enable analysis of samples to go so far as to obtain information in relation to an individual's propensity to commit certain crime and be used for that purpose within the language of the present section. It might also be said that the law might be changed in order to allow the samples to be used for purposes other than those identified by the section. It might also be said that while samples are retained there is even now a risk that they will be used in a way that the law does not allow. So, it is said, the aims could be achieved in a less restrictive manner, and Liberty pose the questions: if other jurisdictions fulfil the same aims with greater safeguards eg judicial scrutiny of decisions to retain samples, why should not this jurisdiction be able to do the same? Why cannot the aim be achieved by retention of the profiles without retention of the samples?

61 The answer to Liberty's points is as I see it as follows. First the retention of samples permits (a) the checking of the integrity and future utility of the DNA database system; (b) a reanalysis for the upgrading of DNA profiles where new technology can improve the discriminating power of the DNA matching process; (c) reanalysis and thus an ability to extract other DNA markers and thus offer benefits in terms of speed, sensitivity and cost of searches of the database; (d) further analysis in investigations of alleged miscarriages of justice; and (e) further analysis so as to be able to identify any analytical or process errors. It is these benefits which must be balanced against the risks identified by Liberty. In relation to those risks, the position in any event is first that any change in the law will have to be itself Convention compliant; second any change in practice would have to be Convention compliant; and third unlawfulness must not be assumed. In my view thus the risks identified are not great, and such as they are they are outweighed by the benefits in achieving the aim of prosecuting and preventing crime.

62 The answer to the first question posed by Liberty is first that the fact that other jurisdictions do things differently cannot provide an automatic answer that this jurisdiction must be in breach of the Convention, and in any event second, judicial scrutiny of the question of whether retention should be allowed does not provide an answer to any of the risks identified by Liberty which occur whether judges have scrutinised the question of retention or whether retention is on the basis provided for by the new section.

63 The answer to the second question is that retention of the samples is beneficial in all the ways identified, and in particular it ensures the integrity

71

and future utility of the database. The benefits outweigh any risks identified. The law is proportionate to the aim being sought to be achieved. That is so because, in the fight against crime, there is the need to be allowed to retain the samples lawfully taken. To keep profiles alone would not be sufficient.

64 As regards article 14, the argument is that the rights under article 8(1) are being secured for some persons and not for others, and that those others are being selected on the basis of "their status". The suggestion is that there is a pool of innocent persons, and that amongst that pool of innocent persons are those acquitted. Thus the argument goes the law discriminates against those innocents with the "status" of having been acquitted. Sedley LJ as I understand it accepts that the relevant pool is as above described, but justifies the retention of samples of those people who have been the subject of investigation, on the basis that not all unconvicted people are equal from a policing point of view, and among those who have been charged but not convicted it is especially so. It is this conclusion which leads him to express the view in paragraph 94, when he deals with the question of discretion, that a Chief Constable should destroy data where he is satisfied on conscientious consideration that the individual is free of any taint of suspicion.

65 I cannot, I am afraid, agree with Sedley LJ. In relation to discrimination the argument depends on defining the pool as all innocent, i e unconvicted, people. So far as this change in the law is concerned, this does not seem to me to be an accurate description of the relevant pool. The situation is not one in which the authorities have samples from all innocent people, and are being given the power to retain only those samples from innocent people who have been suspected of offences but acquitted. Indeed to characterise the pool as being all innocent, i e unconvicted, persons would be quite unfair because there is little doubt that if the authorities had the power to obtain samples from every person, innocent or otherwise, they would not contemplate discriminating against any section of that pool. The bigger the databank the better. The fact that that step has not yet been taken, and the only step being taken is to keep samples lawfully taken, demonstrates to my mind that the relevant pool is that of persons from whom samples have been lawfully taken. Those persons are being treated alike and there is thus in my view no breach of article 14.

66 Furthermore in the context of discretion, to introduce a concept of a Chief Constable having to consider whether a person is free of any taint of suspicion has great difficulties, and as it seems to me is raising a consideration which in fact should not apply at the retention stage. At the retention stage consideration of the circumstances of the *offence* of which the person has by this stage been acquitted seems to me almost certainly irrelevant. I accept that if some form of undertaking were given to destroy to induce a person to co-operate in the taking of a sample, that would be relevant, but the circumstances of the offence itself would as I see it not be. Apart from the "undertaking type case", retention is only relevant to the question whether the details on the databank will assist in either the elimination or the conviction of a person so far as some future criminal investigation is concerned. If justification for retention is in any degree to be by reference to the view of the police on the degree of innocence, then persons who have been acquitted and have their samples retained can justifiably say this stigmatises or discriminates against me—I am part of a

72

pool of acquitted persons presumed to be innocent, but I am being treated as though I was not. It is not in fact in anyway stigmatising someone who has been acquitted to say simply that samples lawfully obtained are retained as the norm, and it is in the public interest in its fight against crime for the police to have as large a database as possible. I accordingly do not subscribe to the view that the Chief Constable is bound to exercise his discretion in the way suggested by Sedley LJ.

SEDLEY LJ

67 In my judgment: (a) the retention of fingerprints and bodily samples taken from unconvicted persons breaches their right to respect for their private life under article 8(1); (b) article 8(2) affords a primary justification; (c) the legislative distinction between unconvicted persons who respectively have and have not been in the hands of the police is objectively justified under articles 8(2) and 14, provided data are destroyed in cases which it turns out should never have been initiated.

Article 8(1)

68 I respectfully agree with Lord Woolf CJ, for the reasons he gives, that while the retention of personal material and data is much less invasive than the taking of them, it nevertheless represents a further and continuing invasion of the right recognised by article 8(1) to respect for one's private life. In reaching this view we are fully entitled to take into account the strong cultural unease in the United Kingdom about the official collection and retention of information about individuals.

Article 8(2)

69 The next question is whether retention of fingerprints or of bodily samples which is permitted under section 64 of PACE is justified under article 8(2). The purposes of retention—the prevention of crime and the protection of the right of others to be free from crime—are four-square within article 8(2), and retention is provided for by law.

70 The question then is whether retention is necessary in a democratic society: that is to say, whether it is a proportionate interference with the primary right to respect for one's private life. Here the critical issue is whether the legitimate purposes can be achieved by less drastic means. For reasons I will come to, I believe that the other large issue, the singling out from the whole of the unconvicted population of those who have been suspects, is most appropriately dealt with under article 14. But it is possible to pose and answer the same questions under article 8(2). I deal with both later.

Fingerprints

71 Fingerprints do not differ in principle from photographs. They are a means of recognising somebody. They differ in practice in that they can only be obtained with the consent of the suspect or by force. But once obtained, they are fixed data, and I find little difficulty in holding that their retention meets a legitimate objective in a way which no less invasive technique can do. I will come under the head of discrimination to the question: why only the fingerprints of former suspects?

73

Bodily samples

72 Bodily samples are also a source of identifying data. The data themselves have a clear and important role both in tracing the guilty and in clearing the innocent. But samples are capable of affording much more than identifying data: how much more we do not know; neither do legislators or the police, for it lies in the scientific future. This is why I have found Liberty's written submission of great assistance. It avoids the polar positions adopted, as tends to happen in litigation, by the parties and instead reasons by degrees. The distinction which Liberty draws between DNA profiles and the bodily samples from which the profiles are derived is in my judgment crucial to what we have to decide. So too are the evidence and written argument submitted in response by the Home Secretary after the close of oral argument, pursuant to the court's direction. But the true parameter of the debate is in my judgment that addressed by Liberty: not what is currently done under section 64 (to which much of the Home Secretary's evidence goes) but what section 64 permits.

DNA profiles

73 As fixed data, DNA profiles are not unlike fingerprints, although what they convey is at once more complex and more comprehensive. Neither science is without inherent weaknesses and risks of human error; but these are for exploration and evaluation in the courtroom. Nobody can rationally doubt the potential utility of DNA profiles both in convicting the guilty and in exonerating the innocent.

DNA samples

74 DNA samples in themselves have no forensic or diagnostic value. Their value lies in the comparative data they yield, and these can be derived and stored without the need to retain the sample. If the reliability of the profile is challenged at a future date, it will be in the subject's interests to provide a fresh sample to resolve the dispute. In any event, on any future arrest a fresh bodily sample will be taken (and Dr Bramley's evidence is that for court purposes and to eliminate profiling error the fresh sample is routinely analysed). This should mean that accidentally transposed profiling, which Dr Bramley candidly admits is a risk, is unable to affect the trial process. So the principal case for retention has to be that science may in the future enable more information to be derived from bodily samples than is possible at present. And this, paradoxically, is also the case against retention.

75 The burden necessarily lies on the state to show that retaining lawfully obtained bodily samples (whether of convicted or of unconvicted persons does not matter here), as opposed to the DNA data the samples yield, will meet a pressing social need in a way which does not disproportionately invade the subject's right to respect for his or her private life. It is the very indeterminacy of the future use of such samples, which may as easily be for ill as for good, which the claimants argue prevents the state from establishing a sufficient justification under article 8(2) for the particular invasion of personal privacy under article 8(1).

76 This is an issue of great importance, but in my judgment it does not advance either side's case under article 8(2). Let us suppose that in 10 years'

74

A time it becomes possible to deduce the propensity of individuals to resort to violence from presently unrecognised elements of their DNA, and that this evidence is made admissible in prosecutions for crimes of violence. The retention of an individual's bodily sample, if section 64 of PACE is now allowed to stand, will have exposed him or her to the possibility of an invasion of his article 8(1) rights which falls outside any justification now capable of being advanced. Whether the individual has been convicted or not, the answer has to be either that (as Lord Woolf CJ holds) the residual discretion implicit in the power must be used to maintain Convention-compliance, or (as I would respectfully hold) that the United Kingdom's legislatures will be required by international obligation to enact Convention-compliant rules—which may include outright prohibition—for new scientific uses of DNA. In this sense, even Parliament's powers are not untrammelled. Meanwhile it is clear that PACE permits no such use. The only alternative is to assume the very thing that the United Kingdom's international obligations forbid, a future transgression of the limits of article 8(2).

77 These considerations do much to resolve the issue of proportionality, an issue which, with respect, I do not think can ever be absorbed in a simple balancing exercise as between the individual and the public (an exercise which in a majoritarian democracy the individual will always lose, and which the Convention is there precisely to redress). Nor does the Human Rights Act 1998 permit it to be resolved by simple deference: in my judgment Parliament has spelt out in sections 3, 4 and 5 of the Act the form and measure of deference which it requires of the courts, and the jurisprudence which section 2 requires us to take into account maintains judicial vigilance without seeking to supplant the democratic process.

78 Exercising the judgment which, in my respectful view, Parliament has confided to the courts, I consider that the means made available by section 64 of PACE to meet what is plainly a pressing social need are limited by law to a practical minimum of intrusion upon the respect owed by the state to the private life of those affected. The rule of law means that they will not open a Pandora's box of unknown uses. The alternative of keeping the profile and destroying the sample is, for the reasons given, neither legally nor factually a significantly less invasive technique.

Discrimination

79 This brings me to what I regard as the most difficult question in the case: out of the whole unconvicted population, what can justify the retention of samples (and the data they yield) taken only from those who have been suspected of crime but not convicted? How can it be squared with the presumption of innocence?

80 This issue of discrimination arises (a) because there must under article 8(2) be a rational connection between the measure and the objective, and arbitrary discrimination is not rational or proportionate (see *Aston Cantlow and Wilmcote with Billesley Parochial Church Council v Wallbank* [2002] Ch 51, 66, para 45); and (b) because Convention rights, by virtue of article 14, must be enjoyed "without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social origin, association with a national minority, property, birth or other status". It seems to me that to have been charged or investigated but not

75

convicted is both as involuntary and as stigmatic a condition as the majority of those listed in article 14, and that it falls sensibly within the catholic phrase "other status". But whichever article it is put under, the point is essentially the same.

81 It is a necessary part of the answer, but not in my respectful view a sufficient one, that what distinguishes them is the fact that they have already had their fingerprints and bodily samples lawfully taken. What in my judgment makes the justification sufficient is that those who have been accused but discharged are not necessarily on a par with those who have never been accused.

82 It is perfectly true that the taking of fingerprints and samples is antecedent to their retention and that its lawfulness, at a time when by definition the suspect is unconvicted, is given and accepted as Convention-compliant. But to make this alone the justification for retention is to assume the very thing which has to be decided, namely whether the grounds for keeping suspects' fingerprints and samples continue to be valid once they have been cleared.

83 The two main grounds for taking fingerprints and bodily samples from persons charged are that they may help in the proof (or disproof) of their involvement in the crime of which they are suspected, and that they may help in the detection of the authorship of other crimes. Once the individual has been discharged, the first of these grounds—save in the rarest cases—is spent. It is the second, the clearing up of other crimes, which gives a ground for retention. But what then is the rational connection between this entirely defensible objective and the use of data only from those of the unconvicted population who have at some time been investigated or faced charges? So long as the unconvicted are all taken to be equally beyond suspicion, the fact that the latter alone have had their fingerprints and samples lawfully taken must be a matter of pure chance and cannot be a legally proper ground of distinction. But is the premise correct?

84 In the eye of the law, everybody is innocent save those who have been lawfully convicted. The principle is not mere cant: it is a real and important bulwark of liberty, and nothing which follows is intended to devalue it. But from a policing and law enforcement point of view the unconvicted population is not uniformly beyond suspicion: it cannot be if policing is to function properly, for detection ordinarily begins not with proof but with inquiry. Of those who come lawfully into the hands of the police in the course of investigation but are not convicted, there will inevitably be some who ought never to have been suspected, much less charged; and others who ought without doubt to have been convicted but for one reason or another have not been. Between these poles lies a range of more or less justified suspicion which for one reason or another has not resulted in a conviction. Among the most common of the latter cases are charges of violent offending which cannot be proceeded with because the victim is afraid to testify. Among the most disturbing are rapists who repeatedly secure acquittals, more than one of whom has finally been caught by matching their DNA with data from other, unsolved rapes. A requirement to destroy DNA profiles on acquittal would have made this impossible.

85 It is here, if anywhere, that one has to find the justification for retaining the fingerprints only of those unconvicted people who have been the subject of investigation. In my judgment it is there. There is of course

76

nothing which says that those who have never been suspected of anything will not offend, nor that those who have already fallen under justified suspicion but have been acquitted will go on to offend; but the courts know well that among the latter is a significant proportion—markedly higher than in the unconvicted population at large—who will offend in the future. Not all unconvicted people, in other words, are equal from a policing point of view, even though they are from a legal one; and among those who have been charged but not convicted it is especially so.

86 Thus it is not right to regard the operation of section 64 as simply a by-product of the misfortune of having been wrongly charged with an offence. The line between those unconvicted people who have faced charges and those who have not, while not a bright line, is not arbitrarily drawn. It does not tarnish the innocence of the unconvicted in the eye of the law. But it recognises that among them is an indeterminate number who are likelier than the rest of the unconvicted population to offend in the future or to be found to have offended in the past. The downside, which is that the same cohort will inevitably include people who never have offended and never will, is in my judgment—given the protective qualification to which I come below—a necessary and reasonable price to pay. It is not a cost which falls directly or perceptibly upon the individuals concerned, and it affords a very important benefit to society.

87 This leaves one further argument to be addressed: if the foregoing reasoning is right, why not a comprehensive (and so non-discriminatory) DNA register, since the arguments for it are the same? For reasons powerfully addressed in the judgment of Lord Woolf CJ, I would certainly not assume that a comprehensive national DNA database or samples bank, if one were to be lawfully compiled, would constitute an unacceptable invasion of privacy. It would be for Parliament to decide whether the intrusion and surveillance involved in assembling and maintaining such a resource is an acceptable price to pay for its advantages. Certainly the information available to this court suggests that, subject to these considerations, a universal DNA register would be a real and worthwhile gain in the endeavour to ensure that the guilty, and only the guilty, are convicted of crimes. In other words, whether it is the unconvicted population as a whole whose bodily samples are kept or only that section of it which has faced charges, the justification is the same.

Discrimination: the "pool"

88 It will be apparent from the judgment of Waller LJ that, had he adopted my view that section 64 introduced discrimination which needed to be justified, he would not have accepted my methodology of justification. This does not matter to the outcome of the present appeals, on which we agree; but it is capable of mattering a great deal in discrimination law generally, and I wish therefore to explain why I respectfully differ from him.

89 There is a logical and consistent concept of indirect discrimination in the statutory formula contained in section 1(1)(b) of the Sex Discrimination Act 1975 and section 1(1)(b) of the Race Relations Act 1976. It reappears, with adaptations, in the Disability Discrimination Act 1995. It was derived from the exegetic concept of indirect discrimination developed by the United States Supreme Court in *Griggs v Duke Power Co* (1971) 401 US 424. It corresponds closely with the jurisprudence of the European Court of Justice

77

(initially in relation to the free movement of goods: *Geitling v High Authority of the European Coal and Steel Community* (Case 2/56) [1957] ECR 3; subsequently across the board in relation to gender equality); with a series of EU Council directives, including the recent Race Directive 2000/78/EC; and with the jurisprudence of the European Court of Human Rights (*Belgian Linguistic Case (No 2)* (1968) 1 EHRR 252). It is therefore of real importance that this court should not adopt a deviant approach.

90 Central to indirect discrimination is the ostensibly neutral factor which on analysis significantly and unjustifiably disadvantages a protected group. *Griggs v Duke Power Co* 401 US 424 provides a well known example: because of educational disadvantage, black workers did significantly worse than white workers in literacy tests which were applied to all employees but were objectively unnecessary. The discriminating factor was not facing the literacy test but failing it. But its differential impact could only be measured in a pool consisting of both white and black workers—that is, both those disadvantaged and those not disadvantaged by it. In the present appeals the discriminating factor is not the fact of having had samples lawfully taken; it is being a person who has had them taken but has not then been convicted. To confine the pool for testing its effect to other people in the identical position, as Waller LJ would do, and to conclude—inexorably—that they are all being treated alike, is the equivalent of confining the pool in the *Griggs* case to black workers. The correct pool in such a case (that is, the pool which will test the particular complaint) is everybody in the same relevant situation: in the *Griggs* case, all the company's workers to whom the test was given; in the present appeals, all citizens who have not been convicted of an offence.

91 To take as your pool simply the group which asserts that it is being discriminated against and to find—as you practically always will—that they are all being treated the same is to defeat the rationale of indirect discrimination. To take as your pool a larger group which does not share the *relevant* characteristic—here, for example, *everyone* who has had their fingerprints and bodily samples lawfully taken—will be to sidestep the legal issue. The legal issue is not (as in another system it might have been) the absence of discrimination between convicted and acquitted suspects: it is the presence of discrimination between legally innocent people who respectively have and have not been investigated.

92 Hence the difference, with very great respect, between my approach and that of Lord Woolf CJ to the question of discrimination. (For a detailed account of the topic, see *Deakin & Morris, Labour Law*, 3rd ed (2001), pp 571–574, and the Legal Action Group's *Discrimination Law Handbook*, 4th ed (2002), ch 7.) There are without doubt situations in which identifying an appropriate pool becomes complex; but this is not one of them. This is why I do not find it possible simply to accept the lawful initial taking of samples as a sufficient justification of their retention, and why I have found it necessary to examine the justification for the distinction which the statute makes between those within the unconvicted population who have been and who have not been investigated by the police.

Conclusion

93 For these reasons, albeit they are not entirely those of the other members of this court or of the Divisional Court, I too would hold that the

78

connection between the retention of the fingerprints and bodily samples of people who have been accused of crime but discharged and the legitimate purpose of combating crime is a rational one; that the relatively modest invasion it involves of their right to respect for their private life is proportionate; and that in so far as the selection of such people from the unconvicted population at large discriminates against them, it is objectively justified.

94 But this carries a qualifying corollary: the very reasoning which holds that retention is ordinarily permissible requires careful regard to be had to that margin of cases where suspicion itself turns out to have been unjustified or, though justified, to have been completely refuted. It is here, in my judgment, that the word "may" in section 64 has a precise significance. The power of a Chief Constable to destroy data which he would ordinarily retain must in my judgment be exercised in every case, however rare such cases may be, where he or she is satisfied on conscientious consideration that the individual is free of any taint of suspicion. Such a person in my judgment falls outside the purposes for which retention is justifiable under the Convention, and the court's obligation under section 3(1) of the Human Rights Act 1998 to read and give effect to primary legislation compatibly with the Convention rights requires us so to construe section 64 of PACE. It is also a reading which seems to me to come closest to producing just outcomes in a problematical field.

95 Since, however, the other two members of the court take a different view of the residual discretion contained in section 64, the Chief Constable will not be required—as I would have required him—to consider whether either of the two cases before the court falls into the category I have described.

Appeals dismissed with costs.
Permission to appeal refused.

Solicitors: Howells, Sheffield; Solicitor for the South Yorkshire Police; Treasury Solicitor.

JBS

79

Icelandic Supreme Court

Thursday 27 November 2003

No. 151/2003.

Ragnhildur Guðmundsdóttir

(Ragnar Aðalsteinsson, Attorney at Law)

vs.

The State of Iceland.

(Skarphéðinn Þórisson, Attorney at Law)

Protection of privacy. The Constitution of Iceland. Medical records. Personal data.

R appealed for a decision by the Court to overturn the refusal of the Medical Director of Health to her request that health information in medical records pertaining to her deceased father should not be entered into the Health Sector Database. Furthermore, she called for recognition of her right to prohibit the transfer of such information into a database. Article 8 of Act No 139/1998 on a Health Sector Database provides for the right of patients to refuse permission, by notification to the Medical Director of Health, for information concerning them to be entered into the Health Sector Database. The Court concluded that R could not exercise this right acting as a substitute of her deceased father, but it was recognised that she might, on the basis of her right to protection of privacy, have an interest in preventing the transfer of health data concerning her father into the database, as information could be inferred from such data relating to the hereditary characteristics of her father which might also apply to herself. It was revealed in the course of proceedings that extensive information concerning people's health is entered into medical records, e.g. medical treatment, life-style and social conditions, employment and family circumstances, together with a detailed identification of the person that the information concerns. It was recognised as unequivocal that the provisions of Paragraph 1 of Article 71 of the Constitution applied to such information and guaranteed to every person the right to protection of privacy in this respect. The Court concluded that the opinion of the District Court, which, inter alia, was based on the opinion of an assessor, to the effect that so-called one-way encryption could be carried out in such a secure manner that it would be virtually impossible to read the encrypted data, had not been refuted. It was noted, however, that Act No. 139/1998 provides no details as to what information from medical records is required to be encrypted in this manner prior to transfer into the database or whether certain information contained in the medical records will not be transferred into the database. The documents of the case indicate that only the identity number of the patient would be encrypted in the database, and that names, both those of the patient and his relatives, as well as the precise address, would be omitted. It is obvious that information on these items is not the only information appearing in the medical records which could, in certain cases, unequivocally identify the person concerned. Act No. 139/1998 also provides for authorisation to the licensee to process information from the medical records transferred into the database. The Act stipulates that certain specified public entities must approve procedures and process methods and monitor all queries and processing of information in the database. However, there is no clear definition of what type of queries will be directed to the database or in what form the replies to such queries will appear. The Court concluded that even though

individual provisions of Act No 139/1998 repeatedly stipulate that health information in the Health Sector Database should be non-personally identifiable, it is far from adequately ensured under statutory law that this stated objective will be achieved. In light of the obligations imposed on the legislature by Paragraph 1 of Article 71 of the Constitution, the Court concluded that various forms of monitoring of the creation and operation of the database are no substitute in this respect without foundation in definite statutory norms. In light of these circumstances, and taking into account the principles of Icelandic law concerning the confidentiality and protection of privacy, the Court concluded that the right of R in this matter must be recognised, and her court claims, therefore, upheld.

Decision of the Supreme Court

Presiding in the case are Supreme Court Judges Guðrún Erlendsdóttir, Garðar Gíslason, Gunnlaugur Claessen, Markús Sigurbjörnsson and Pétur Kr. Hafstein.

The Appellant referred the case to the Supreme Court on 29 April 2003, calling for a reversal of the refusal of the Medical Director of Health to her request of 16 February 2000 to the effect that information from the medical records of her father, Guðmundur Ingólfsson, who died on 12 August 1991, should not be transferred into the Health Sector Database. The Appellant furthermore calls for the Court's recognition of her right to prohibit the transfer of the above information into the database. She also claims costs before the District Court, notwithstanding the legal aid provided to her before the present Court.

The Defendant calls for confirmation of the decision of the District Court and payment of costs before the Supreme Court.

I.

The Health Sector Database Act No. 139/1998 entered into force on 30 December 1998. According to Article 1 of the Act, the purpose of the Act is to authorise the creation and operation of a centralised database of non-personally identifiable health data, with the aim of increasing knowledge for the purpose of improving health and health services. Article 4 lays down the condition that authorisation for such operation is subject to an operating licence, for which conditions are laid down in Article 5 of the Act. Article 6 of the Act entrusts a specially appointed committee with the supervision of the creation and operation of the database to the extent that this does not fall within the terms of reference of the Data Protection Authority, which works on the basis of Act No. 77/2000 on the Protection of Individuals with regard to the Processing of Personal Data. Article 7 of Act No. 139/1998 contains instructions on the authorisation of the licensee to obtain data

derived from the medical records of health institutions and self-employed health service workers. However, according to Article 8, persons who do not want information on them to be entered into the database can prevent this by a notification to the Medical Director of Health. Article 10 of the Act contains instructions concerning the utilisation of the database, including the purpose, restrictions and supervision, Article 11 provides for the obligation of confidentiality of the employees of the licensee and contractors in his service, while Article 12 contains further instructions on monitoring by the Data Protection Authority, the Committee on the Operation of the Database referred to above, and the so-called Multidisciplinary Ethics Committee. Finally, Chapter VI of the Act contains rules on the withdrawal and revocation of licenses, sanctions and damages.

The Minister of Health and Social Security issued Government Regulation No. 32/2000 on a Health-Sector Database on 22 January 2000. On the same date, the Minister issued a license to Íslensk Erfðagreining ehf. for the creation and operation of the Health Sector Database. The license was accompanied by seven annexes containing, first, General Specifications for Medical records Systems intended for use in medical institutions in connection with the reporting of information to the database, and second, Rules on the Transfer of Data. Third, it contained a summary of the Main Formal and Substantive Aspects of Agreements between the Licensee and Health Institutions and Self-Employed Health Service Workers, concerning access to the information contained in medical records. Fourth, it contained a Status Report on Health Data with the minimum requirements for databases and information systems. Fifth, it contained Terms of Financial Separation in the operation of the licensee between the departments concerned with the Health Sector Database and other departments in his operation, and sixth, a Register of Health-Care Professions permitted to record and process information for transfer into the database. Seventh, and last, the licence was accompanied by a document on the Technology, Safety and Organisation Terms of the Data Protection Commission for the database; the tasks of that Commission, however, have now been taken over by the Data Protection Authority.

The guardian of the Appellant, who was born in 1985, wrote a letter to the Medical Director of Health on 16 February 2000, with an enclosed notification in the Appellant's name requesting that information contained in her father's medical records should not be transferred to the Health Sector Database. Furthermore, the request was

made that the genealogical or genetic information on the Appellant's father should not be transferred into the database. The Medical Director of Health replied by a letter dated 21 February 2001. Reference was made, *inter alia*, to the fact that Act No. 139/1998 contained no direct provisions on the right of the relatives of a deceased person to prevent information about him/her being transferred into the Health Sector Database. However, in the commentary attached to the legislative Bill which eventually passed into law it had been stated that it was not the intention that people should be able to refuse the transfer of information on their deceased parents into the database. The Medical Director of Health had obtained a legal opinion concerning this matter, which he enclosed with his reply. Based on this opinion he said that he could not comply with the Appellant's request.

Following receipt of the reply of the Medical Director of Health, the Appellant initiated these proceedings on 30 April 2001. Two of Guðmundur Ingólfsson's sons have declared in writing that they consent to the proceedings and there is no evidence from the parties that he left any other children apart from these.

Based on information that emerged in the course of proceedings before the Supreme Court, the compilation of the Health Sector Database has not yet started. There is, furthermore, some doubt that this will happen. The documents of the case do not reveal that formal measures for the preparation of the database have advanced significantly since the operating license was issued on 22 January 2000 to Íslensk Erfðagreining ehf. and the annexes to the license referred to above were ready.

II.

According to the principles of Icelandic law, the personal rights of individuals lapse on their death insofar as legislation does not provide otherwise. The previously mentioned Article 8 of Act No 139/1998 does not provide for the right of descendants or other relatives of deceased persons to request, on their behalf, that information in their medical records should be withheld from the Health Sector Database. No such rule can be inferred from any other sources of law. The Appellant cannot, therefore, exercise the right provided for in this statutory provision as her deceased father's substitute.

As stated in the appealed judgement, the Appellant bases her legitimate interest in the case partly on the fact that she has a personal interest in preventing the transfer of data from her father's medical records to the Health Sector Database, as it is possible to infer, from the data, information relating to her father's hereditary

characteristics which could also apply to herself. The Defendant has not submitted to the court any expert testimony to rebut this contention of the Appellant. In light of this, and with reference in other respects to the reasoning of the District Court, the argument of the Appellant is accepted that, for reasons of personal privacy, she may have an interest in preventing information of this sort about her father from being transferred into the database, and therefore her right to make the claims that she is making in the case is admitted.

III.

Paragraph 2 of Article 2 of Regulation No. 227/1991 on Medical records and Reporting of Health Issues, as amended by Article 1 of Regulation No. 545/1995, includes rules concerning the data on the person and circumstances of a patient that should be included in medical records. According to Item 1 of the provision these should include the name of the patient, address, telephone number, identity number, professional title, marital status and next of kin. Item 3 states that entries into the medical record should include medical history, including information on diet, use of medicines, allergies to medicinal products, use of tobacco, alcohol and other intoxicants. According to Item 4 of the provision, an account should also be given of the family and social circumstances of the patient. In addition, there is an itemised list in ten numbered points concerning illness, medical treatment, subsequent course of events and physicians' reports, which should be accounted for in the medical records at any time. This regulation was passed on the basis of Articles 16 and 18 of the Medical Act No. 53/1988, as current at the time. Those provisions were amended by Acts No. 76/1997 and No. 68/1998, so that they no longer seem to provide any basis for the regulation. In the course of oral pleadings before the Supreme Court, however, the Defendant stated his opinion that the regulation was still in effect, and this contention is supported in part by Article 29 of Act No 74/1997 on Patients' Rights.

According to Paragraph 1 of Article 7 of Act No. 139/1998, it is permitted, with the approval of health institutions or self-employed health service workers, to provide data processed from medical records to the holder of an operating licence for a health sector database for transfer into the database. Health institutions shall consult with their physicians' council and professional managers before negotiating contracts with the licensee. Paragraph 2 of Article 7 of the Act states that the handling of records, other documents and information shall comply with the conditions regarded as necessary by the Data Protection Authority at any time. Personal identifiers must be

encrypted by means of one-way coding, as defined in Items 4 and 5 of Article 3 of the Act, before the information is transferred into the database, in order to ensure that the licensee's staff only work with non-personally identifiable data. Health institution staff or self-employed health service workers must prepare the data for transfer into the database and the data must be transported in encrypted form. The Data Protection Authority is entrusted with the further encryption of personal identifiers using the methods regarded by the Authority as best suited to ensure the protection of personal privacy. Provisions on these matters are also contained in Regulation No. 32/2000, mentioned earlier, particularly Articles 9, 31 and 33, as well as in Article 16 on the form of agreements between the licensee and health institutions and self-employed health service workers. These do not delimit in further detail what information from medical records may be transferred into the Health Sector Database. This, however, is described to some extent in the previously mentioned annex to the operating license issued to Íslensk Erfðagreining ehf., which concerns the transfer of information into the Health Sector Database, although in this respect a distinction is drawn between information entered into medical records prior to the introduction of a harmonised electronic system of medical records and information entered after the introduction of such a system.

Article 10 of Act No. 139/1998 provides that data recorded in the Health Sector Database, or obtained by processing in the database, may be used to develop new or improved methods of achieving better health, prediction, diagnosis and treatment of diseases, to seek the most economic ways of operating health services, and to produce public health reports. The licensee is authorised to process data in the database from the medical records therein, provided that data are processed and connected in such a way that they cannot be traced to identifiable individuals. The obligation is imposed on the licensee to develop methods and protocols that meet the requirements of the Data Protection Authority in order to ensure protection of privacy in connecting data from the Health Sector Database, from a database of genealogical data, and from a database of genetic data. It is stated specifically in the provision that no information on individuals must be given, and this shall be ensured by means which include access restrictions. Also, the licensee is not permitted to provide direct access to data in the database. According to Paragraph 1 of Article 12 of the Act, the Data Protection Authority is responsible for monitoring the creation and operation of the database with regard to the recording and handling of personal data and the security of data in the

database, and it is also responsible for monitoring compliance with conditions laid down by the Authority. The Committee on the Operation of the Database, mentioned above, is entrusted, in Paragraph 2 of the same Article, with monitoring the full compliance of the operation of the database with the provisions of the Act, regulations issued thereunder and the conditions of the operating licence. The committee is moreover responsible for monitoring all queries and processing of information from the database and also for reporting regularly to the National Bioethics Committee on all queries processed in the database and the sources of the queries. Moreover, Paragraph 3 of Article 12 of the Act provides for the obligation of the Minister to issue a regulation on an multidisciplinary ethics committee to evaluate licensee's research and queries to the database. According to the Act, the committee's evaluation must show that there are no scientific or ethical grounds for preventing the study in question from being carried out or for preventing the queries from being processed. The issues discussed here are also addressed in provisions in Articles 13, 14, 21, 26, 28 and 32 of Regulation No. 32/2000. However, it is not delimited in any significant further detail what type of queries will be addressed to the database or what form the replies to such queries will take with or without links with the database containing genealogical or genetic data. In the oral pleadings before the Supreme Court the Defendant stated that responses from the database would only have the form of statistical and completely non-personally identifiable data, although no rules had yet been issued and no decisions made concerning the further details of this matter.

IV.

As may be inferred from the above, extensive information is entered into medical records on people's health, their medical treatment, lifestyles, social circumstances, employment and family. They contain, moreover, a detailed identification of the person that the information concerns. Information of this kind can relate to some of the most intimately private affairs of the person concerned, irrespective of whether the information can be seen as derogatory for the person or not. It is unequivocal that the provisions of Paragraph 1 of Article 71 of the Constitution apply to information of this kind and that they guarantee protection of privacy in this respect. To ensure this privacy the legislature must ensure, *inter alia*, that legislation does not result in any actual risk of information of this kind involving the private affairs of identified persons falling into the hands of parties who do not have any

legitimate right of access to such information, irrespective of whether the parties in question are other individuals or governmental authorities.

Article 7 of Act No. 139/1998 opens the possibility of a private entity, who is neither a medical institution nor a self-employed health service worker, obtaining information from medical records without the explicit consent of the person whom the information concerns. Although this alone does not necessarily, in and of itself, violate the provisions of Paragraph 1 of Article 71 of the Constitution, the legislature, having regard to all of the above, must take steps, in the establishment of a rule of this kind, to ensure to the furthest extent that the information cannot be traced to specific individuals. The District Court, where the Bench included an assessor, concluded that the so-called one-way encryption discussed in Item 5 of Article 3 of Act No. 139/1998, could be carried out so securely as to render it virtually impossible to read the encrypted information. This conclusion has not been contested successfully in the course of the proceedings before the Supreme Court. It should be noted, however, that Act No. 139/1998 provides no guidance as to what information from medical records must be encrypted in this manner prior to transfer into the Health Sector Database or whether certain information contained in the medical records relating to the personal identity of the patient will not be transferred. Nor is this issue addressed in Regulation No. 32/2000. The annex to the operating licence issued to Íslensk erfðagreining ehf., mentioned earlier, which concerns the transfer of information to the Health Sector Database, appears to imply that only the identity number of the patient will be encrypted in the database and that the name, both of the patient and his family, together with the precise address will be omitted. It is obvious that information on these items is not the only information appearing in the medical records which could unequivocally identify the individual in question. In this regard, information concerning the age of a person, municipality of residence, marital status, education and profession, together with the specification of a particular disease, either all together or individually, might suffice. The law does not preclude the transfer of detailed information concerning these items into the Health Sector Database.

The provisions of Article 10 of Act 139/1998 discussed earlier do not specify what information from the medical records involving the personal identifiers of a patients which could be transferred into the Health Sector Database might be seen by a person receiving a response to a query submitted to the database. Nor are there any indications what overall picture could be gained in this respect from the connection of

information from the Health Sector Database with databases containing genealogical information and genetic information, as discussed in the provision. Instead, it is merely provided that steps should be taken in the processing of information to preclude linking of the information with identifiable individuals. There are no further provisions on this in Regulation No. 32/2000. As mentioned earlier, no further plans are available concerning the actual implementation of this in the operation of the Health Sector Database.

Individual provisions in Act No. 139/1998 refer repeatedly to the fact that health information in the Health Sector Database should be non-personally identifiable. In light of the rules discussed above concerning the issues addressed in Articles 7 and 10 of the Act, however, the achievement of this stated objective is far from being adequately ensured by the provisions of statutory law. Owing to the obligations imposed on the legislature by Paragraph 1 of Article 71 of the Constitution to ensure protection of privacy, as outlined above, this assurance cannot be replaced by various forms of monitoring of the creation and operation of the Health Sector Database, monitoring which is entrusted to public agencies and committees without definite statutory norms on which to base their work. Nor is it sufficient in this respect to leave it in the hands of the Minister to establish conditions in the operating licence or appoint other holders of official authority to establish or approve rules of procedure concerning these matters, which at all levels could be subject to changes within the vague limits set by the provisions of Act No. 139/1998.

Article 8 of Act No. 139/1998 permits those who so wish to issue binding instructions to the effect that information about them should not be transferred from medical records into the Health Sector Database. In this way, those who, *inter alia*, may consider their right to protection of privacy threatened by this treatment of information are given the option of taking measures. It has been recognised above that the Appellant may herself have an interest in preventing the transfer of information from her father's medical records into the Health Sector Database because of the risk that inferences could be made from such information which could concern her private affairs. Based on the above, it is impossible to maintain that the provisions of Act No. 139/1998 will adequately ensure, in fulfilment of the requirements deriving from Paragraph 1 of Article 71 of the Constitution, attainment of the objective of the Act of preventing health information in the database from being traceable to individuals. Article 8 of Act No. 139/1998 neither provides for nor precludes a person in the

position of the Appellant requesting that information from the medical records of a deceased parent should not be transferred into a health sector database. In light of this, and taking into account the principles of Icelandic legislation concerning protection of privacy, the Court recognises the right of the Appellant in this respect. Her court claims in this regard are therefore upheld.

In light of this conclusion of the case, the Defendant is ordered to pay the Appellant costs before the District Court and the Supreme Court, which will be determined in one sum as stated in the adjudication. For this reason there is no reason for any ruling on legal aid from the Defendant.

Adjudication:

The decision of the Medical Director of Health to deny the request of Ragnhildur Guðmundsdóttir, dated 16 February 2000, that information from the medical records of Guðmundur Ingólfsson, who died on 12 August 1991, should not be entered into the Health Sector Database, is reversed. The right of the Appellant to prohibit the transfer of this information into the database is upheld.

The Defendant, the State of Iceland, shall pay to the Appellant a total of ISK 1,500,000 in costs before the District Court and the Supreme Court.

House of Lords

*Regina (S) *v* Chief Constable of the South Yorkshire Police

Regina (Marper) *v* Chief Constable of the South Yorkshire Police

[2004] UKHL 39

2004 June 21, 22; July 22

Lord Steyn, Lord Rodger of Earlsferry, Baroness Hale of Richmond, Lord Carswell and Lord Brown of Eaton-under-Heywood

Police — Powers — Retention of evidence — Police taking fingerprints and DNA samples from claimants during course of criminal investigations — Claimants subsequently acquitted or not proceeded against — Police retaining fingerprints and samples — Whether compatible with claimants' rights to privacy and not to be discriminated against — Whether policy of retention lawful — Police and Criminal Evidence Act 1984 (c 60), s 64(1A) (as substituted by Criminal Justice and Police Act 2001 (c 16), s 82) — Human Rights Act 1998 (c 42), Sch 1, Pt I, arts 8, 14

The claimant in the first case, an 11-year-old boy, was arrested and charged with attempted robbery and his fingerprints and DNA samples were taken. He was subsequently acquitted. The claimant in the second case was arrested and charged with harassment and his fingerprints and DNA samples were taken. The Crown Prosecution Service subsequently discontinued the case against him. The police wrote to both claimants informing them that under section 64(1A) of the Police and Criminal Evidence Act 1984, as amended[1], the police had the right to retain fingerprints and DNA samples to aid the investigation of crime and that all such fingerprints and samples would be retained. The claimants sought judicial review on the grounds that the retention of their fingerprints and samples, when they had not been convicted of a criminal offence, was incompatible with their right to privacy under article 8 and their right not to be discriminated against under article 14 of the Convention for the Protection of Human Rights and Fundamental Freedoms, as scheduled to the Human Rights Act 1998[2], and that a general policy of retention was an unlawful fetter on the discretion of the respondent Chief Constable. The Divisional Court dismissed the applications, and the Court of Appeal dismissed the claimants' appeals.

On appeals by the claimants—

Held, dismissing the appeals, that in so far as the retention of fingerprints and DNA samples under section 64(1A) of the 1984 Act constituted an interference with the appellants' right to respect for their private lives under article 8(1) of the Convention such interference was modest and was objectively justified under article 8(2) as being necessary for the prevention of crime and the protection of the rights of others; that the difference in treatment between the appellants and those who had not been required to provide fingerprints and samples was not on the ground of "other status" within article 14 and not on a proscribed ground of discrimination under that article; and that, since it would be unrealistic and impractical to require the police to examine each case individually, a policy of retaining fingerprints and samples of all those who had been required to provide them was lawful (post, paras 31, 36, 40, 50–51, 56, 58–63, 67, 79–80, 84–85, 89).

[1] Police and Criminal Evidence Act 1984, s 64, as amended: see post, para 3.
[2] Human Rights Act 1998, Sch 1, Pt I, art 8: see post, para 6.
Art 14: see post, para 6.

Decision of the Court of Appeal [2002] EWCA Civ 1275; [2002] 1 WLR 3223; [2003] 1 All ER 148 affirmed.

The following cases are referred to in their Lordships' opinions:

Attorney General's Reference (No 3 of 1999) [2001] 2 AC 91; [2001] 2 WLR 56; [2001] 1 All ER 577, HL(E)

Campbell v MGN Ltd [2004] UKHL 22; [2004] 2 WLR 1232; [2004] 2 All ER 995, HL(E)

Friedl v Austria (1995) 21 EHRR 83

Ghaidan v Godin-Mendoza [2004] UKHL 30; [2004] 3 WLR 113, HL(E)

Kinnunen v Finland (Application No 24950/94) (unreported) 15 May 1996, ECommHR

Kjeldsen, Busk Madsen and Pedersen v Denmark (1976) 1 EHRR 711

Leander v Sweden (1987) 9 EHRR 433

McKerr, In re [2004] UKHL 12; [2004] 1 WLR 807; [2004] 2 All ER 409, HL(E)

McVeigh, O'Neill and Evans v United Kingdom (1981) 5 EHRR 71

R v Dyment [1988] 2 SCR 417; 45 CCC (3d) 244

R (Carson) v Secretary of State for Work and Pensions [2002] EWHC 978 (Admin); [2002] 3 All ER 994; [2003] EWCA Civ 797; [2003] 3 All ER 577, CA

R (Ullah) v Special Adjudicator [2004] UKHL 26; [2004] 3 WLR 23, HL(E)

Silver v United Kingdom (1983) 5 EHRR 347

Wandsworth London Borough Council v Michalak [2002] EWCA Civ 271; [2003] 1 WLR 617; [2002] 4 All ER 1136, CA

The following additional cases were cited in argument:

Aston Cantlow and Wilmcote with Billesley Parochial Church Council v Wallbank [2001] EWCA Civ 713; [2002] Ch 51; [2001] 3 WLR 1323; [2001] 3 All ER 393, CA

Brown v Stott [2003] 1 AC 681; [2001] 2 WLR 817; [2001] 2 All ER 97, PC

Handyside v United Kingdom (1976) 1 EHRR 737

Inland Revenue Comrs v Maple & Co (Paris) Ltd [1908] AC 22, HL(E)

Matadeen v Pointu [1999] 1 AC 98; [1998] 3 WLR 18, PC

R v Local Authority and Police Authority in the Midlands, Ex p LM [2000] 1 FLR 612

R v Mitchell (Sean) The Times, 8 July 2004, CA

R (Waite) v Hammersmith and Fulham London Borough Council [2002] EWCA Civ 482; [2003] HLR 24, CA

APPEALS from the Court of Appeal

These were appeals by the claimants, S, by his mother and litigation friend JB, and Michael Raymond Marper, by leave of the House of Lords (Lord Bingham of Cornhill, Lord Scott of Foscote and Lord Rodger of Earlsferry) given on 4 February 2003 from the decision of the Court of Appeal (Lord Woolf CJ, Waller and Sedley LJJ) on 12 September 2002 dismissing appeals by the claimants from the decision of the Divisional Court of the Queen's Bench Division (Rose LJ and Leveson J) on 22 March 2002. The Divisional Court [2002] EWHC 478 (Admin) had dismissed claims by the claimants for judicial review of the policy of the defendant, the Chief Constable of the South Yorkshire Police, to retain the fingerprints and samples of all persons who had been investigated in connection with an offence but who, subsequently, had not been prosecuted for, or had been cleared of, the offence.

The facts are stated in the opinion of Lord Steyn.

Richard Gordon QC, Stephen Cragg and *Benjamin Narain* for the claimants.

Rabinder Singh QC and *James Strachan* for the Secretary of State for the Home Department as an interested party.

David Bean QC, David N Jones and *Garreth Wong* for the Chief Constable.

Their Lordships took time for consideration.

22 July. LORD STEYN

1 My Lords, it is of paramount importance that law enforcement agencies should take full advantage of the available techniques of modern technology and forensic science. Such real evidence has the inestimable value of cogency and objectivity. It is in large measure not affected by the subjective defects of other testimony. It enables the guilty to be detected and the innocent to be rapidly eliminated from inquiries. Thus in the 1990s closed circuit television ("CCTV") became a crime-prevention strategy extensively adopted in British cities and towns. The images recorded facilitate the detection of crime and prosecution of offenders. Making due allowance for the possibility of threats to civil liberties, this phenomenon has had beneficial effects.

2 The use of fingerprint evidence in this country dates from as long ago as 1902. In due course other advances of forensic science followed. But the dramatic breakthrough was the use of DNA techniques since the 1980s. The benefits to the criminal justice system are enormous. For example, recent Home Office statistics show that while the annual detection rate of domestic burglary is only 14%, when DNA is successfully recovered from a crime scene this rises to 48%. It is, of course, true that such evidence is capable of being misused and that courts must be ever watchful to eliminate risks of human error creeping in. But as a matter of policy it is a high priority that police forces should expand the use of such evidence where possible and practicable.

I. Retention of fingerprints and samples

3 It is not in doubt that the *taking* of fingerprints and samples from persons suspected of having committed relevant offences is a reasonable and proportionate response to the scourge of serious crime. What the present appeals are concerned with is the *retention* of such material in cases when a suspect is subsequently acquitted or the charge is discontinued. Until the coming into effect on 11 May 2001 of section 82 of the Criminal Justice and Police Act 2001, the retention by the police of such fingerprints and samples was unlawful under section 64 of the Police and Criminal Evidence Act 1984 ("PACE"). There was public disquiet that this rule sometimes enabled defendants who had in all likelihood committed grave crimes to walk free. Parliament decided to reverse it. Section 64(1A) of PACE, as substituted by section 82 of the 2001 Act, authorises the retention of such fingerprints and samples. It provides:

> "Where—(a) fingerprints or samples are taken from a person in connection with the investigation of an offence, and (b) subsection (3) below does not require them to be destroyed, the fingerprints or samples

A may be retained after they have fulfilled the purposes for which they were taken but shall not be used by any person *except for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution.*" (Emphasis supplied.)

This statutory provision lies at the heart of the present appeals. Its effect is that if a match is made between a fingerprint or a sample found at a crime B scene and a fingerprint or sample taken from an individual before he was cleared of an earlier offence, the police will be able to use the underlying information in the investigation of the offence. It can play a significant role in the elimination of the innocent, the correction of miscarriages of justice and the detection of the guilty.

C *II. The explanatory notes*

4 The mischief against which section 64(1A) is aimed is set out in the explanatory notes which, in accordance with the system introduced in 1999, accompanied the Criminal Justice and Police Bill in its progress through Parliament. Explanatory notes are not endorsed by Parliament. On the other hand, in so far as they cast light on the setting of a statute, and the D mischief at which it is aimed, they are admissible in aid of construction of the statute. After all, they may potentially contain much more immediate and valuable material than other aids regularly used by the courts, such as Law Commission Reports, Government Committee reports, Green Papers, and so forth. The explanatory notes relating to what became the new section 64(1A) read:

E "186. An additional measure has been included to allow all lawfully taken fingerprints and DNA samples to be retained and used for the purposes of prevention and detection of crime and the prosecution of offences. This arises from the decisions of the Court of Appeal (Criminal Division) in *R v Weir* (unreported) 26 May 2000 and *Attorney General's Reference (No 3 of 1999)* [2001] 2 AC 91. These raised the issue of whether the law relating to the retention and use of DNA samples on F acquittal should be changed. In these two cases compelling DNA evidence that linked one suspect to a rape and the other to a murder could not be used and neither could be convicted. This was because at the time the matches were made both defendants had either been acquitted or a decision made not to proceed with the offences for which the DNA profiles were taken. Currently section 64 of PACE specifies that G where a person is not prosecuted or is acquitted of the offences the sample must be destroyed and the information derived from it can not be used. The subsequent decision of the House of Lords overturned the ruling of the Court of Appeal. The House of Lords ruled that where a DNA sample fell to be destroyed but had not been, although section 64 of PACE prohibited its use in the investigation of any other offence, it did not make evidence obtained as a failure to comply with that prohibition H inadmissible, but left it to the discretion of the trial judge. The Bill removes the requirement of destruction and provides that fingerprints and samples lawfully taken on suspicion of involvement in an offence or under the Terrorism Act 2000 can be used in the investigation of other offences. This new measure will bring the provisions of PACE for dealing

with fingerprints and DNA evidence in line with other forms of evidence." A

The light cast on the interpretation of section 64(1A) by the notes is limited but it does show exactly what problem Parliament was addressing.

5 The reference in the explanatory notes to fingerprints is readily intelligible. But it is necessary to make clear what DNA evidence is. The Forensic Science Service on its website under the legend "What is DNA?" B give a simple and useful explanation. So far as material it reads:

"DNA stands for deoxyribonucleic acid. DNA is the chemical which is found in virtually every cell in the body and which carries genetic information from one generation to the next. The genetic information carried in DNA is in the form of a code or language which, when translated, determines our physical characteristics and directs all the C chemical processes in the body. Except for identical twins, each person's DNA is unique. Half of the DNA is inherited from our father and the other half from our mother. DNA can be extracted from any cells that contain a structure called the nucleus. This includes blood, semen, saliva or hair samples."

D

To this general description it is necessary to add that in the present appeal a distinction has been drawn between DNA samples and DNA profiles derived from the samples. Dr Bramley, Chief Scientist of the Forensic Science Service and Custodian of the National DNA Database, explained in a witness statement:

"The samples consist of what is taken by the police under PACE, and E any sub-samples or part samples retained from these after analysis. The DNA profiles are digitised information and it is this digitised information that is stored electronically on the National DNA Database together with details of the person to whom it relates."

III. The questions

F

6 The principal question before the House concerns the compatibility of section 64(1A) with the European Convention on Human Rights as scheduled to the Human Rights Act 1998, and in particular with the Convention rights contained in articles 8 and 14. Respectively these articles provide:

G

"*Article 8*

"*Right to respect for private and family life*

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

"2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is H necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

A "*Article 14*

"*Prohibition of discrimination*

"The enjoyment of the rights and freedoms set forth in this Convention shall be secured without discrimination on any ground such as sex, race, colour, language, religion, political or other opinion, national or social
B origin, association with a national minority, property, birth or other status."

In addition there is a separate question whether the policy of the Chief Constable to retain, save in exceptional circumstances, fingerprints and samples of acquitted individuals in all cases is lawful and compatible with the fundamental rights of individuals.

C *IV. The value of such real evidence*

7 The value of retained fingerprints and samples taken from suspects who were subsequently acquitted is considerable. This is graphically illustrated by a real case which has been referred to as "I". In 1999 a rape and robbery took place. The perpetrator was not known to the victim.
D DNA was recovered from the semen on the victim. A search of the national database showed that the DNA matched that of "I". The sample should have been destroyed. It was not. Following the decision of the House of Lords in *Attorney General's Reference (No 3 of 1999)* [2001] 2 AC 91 the prosecution went ahead. "I" pleaded guilty to rape and was sentenced to a term of seven years (subsequently reduced on appeal to six years) in a young offender institution. But for the wrongly retained sample the offender might
E have escaped detention, possibly to commit other serious crimes.

8 This is one concrete illustration of the value of such evidence. It is part of a broader picture. DNA can be detected from very small samples (such as might be found on the saliva on a cigarette end). The power of this technique to eliminate those suspected or to incriminate others is enormous. The Court of Appeal had before it statistical evidence from Dr Bramley,
F which demonstrated the value of such evidence. In a witness statement of 16 July 2002 he said:

"*Matches with profiles retained under the new provisions of the Criminal Justice and Police Act 2001.*

"To date, approximately 1,700 offences have been detected involving over 1,000 offenders that might have otherwise gone undetected using
G profiles that would previously have been removed from the database prior to implementation of the Criminal Justice and Police Act 2001. These include five murders, nine attempted murders, 23 rapes, six other sexual offences, 15 aggravated burglaries, 14 the supply of controlled drugs and a number of serious assaults"

Two years later Dr Bramley updated the statistics. The effect is summarised
H in the printed case of the Home Secretary:

"As at 31 March 2004, the total number of DNA profiles on the DNA database which relates to entries where the parent PNC records has been deleted is 162,433. It is estimated that approximately 86% of the PNC [Police National Computer] record deletions are attributable to

subsequent acquittals. Allowing for an 8% replication rate among acquittals (for example, reflecting dual entries through use of aliases, etc), it is estimated that there are approximately 128,517 DNA profiles on the DNA database which would previously have been required to be deleted. From these, approximately 5,922 DNA profiles have linked with crime scene stain profiles in respect of 6,280 offences. These offences include 53 murders, 33 attempted murders, 94 rapes, 38 sexual offences, 63 aggravated burglaries and 56 offences of the supply of controlled drugs."

The Home Office statistics show that there is a 40% chance that a crime scene sample will be matched immediately with an individual's profile on the database. These statistics show that fingerprints and samples, which may under section 64(1A) be retained, have in the last three years played a major role in the detection and prosecution of serious crime.

9 This is the context in which the questions before the House must be considered.

V. The two cases before the House

10 There are two appeals before the House. Neither appeal involves an unusual set of facts. They can be regarded as appropriate test cases to consider the questions of law involved.

S

11 When he was arrested on 19 January 2001 S was an 11-year-old boy. He has no previous convictions, cautions or warnings. He was charged with the offence of attempted robbery. Fingerprints and samples were taken from him. Following a trial on 14 June 2001, S was acquitted of the charge. On 18 July 2001, the principal fingerprint officer of South Yorkshire Police wrote to the solicitors acting on behalf of S in these terms:

"I wish to inform you that the South Yorkshire Police will retain fingerprints and samples that were previously required to be destroyed under section 64 of the Police and Criminal Evidence Act 1984. The Criminal Justice and Police Act 2001 now gives the police the right to retain fingerprints and samples to aid crime and investigation and is retrospective. All fingerprints and samples that were due for destruction will be retained."

Then followed further correspondence between the solicitors for S and the South Yorkshire Police in which the solicitors demanded the destruction of the fingerprints and samples of S and the police refused to do so. It is unnecessary to summarise the rival legal contentions of the parties. On 12 October 2001, S sought judicial review of the decision of the police. The standard form N461 summarised the relief sought as follows:

"(1) Quashing order to quash the policy to retain fingerprints and samples in all cases. (2) A declaration that the [Chief Constable] has acted in a manner incompatible with [S's] Convention rights pursuant to article 8 and article 14 of the Convention. (3) A mandatory order to enforce the destruction of [S's] fingerprints and samples. (4) A declaration that section 64 of PACE (as amended) is incompatible with article 8 and

article 14 of the Convention to the extent that it permits the retention of fingerprints and samples of persons with no criminal record."

Mr Marper

12 On 13 March 2001, Mr Marper (who was then 38 years of age and of good character) was arrested and charged with harassment of his partner. The police took his fingerprints and samples. When he appeared in court he pleaded not guilty. The court adjourned his case for a pre-trial review. By the time of that hearing, his partner had become reconciled with him and decided not to press the charge. On 11 June 2001, the Crown Prosecution Service wrote to his solicitors enclosing a notice of discontinuance. On 14 June the case was formally discontinued by the magistrates' court.

13 There was correspondence between the solicitors for Mr Marper and the South Yorkshire Police in which the former demanded destruction of his fingerprints and samples and the police refused to do so. Again the rival legal contentions need not be set out. On 12 December 2001, Mr Marper applied for judicial review of the decision of the police. The application was based on the same legal grounds as those advanced by S.

VI. The Divisional Court

14 The applications for judicial review came before the Divisional Court (Rose LJ (the Vice-President of the Court of Appeal (Criminal Division)) and Leveson J). The judgment was given by Leveson J with the agreement of Rose LJ. The court held that the retention of the fingerprints and DNA samples of individuals who had not been convicted of a criminal offence did not contravene either the individual's right to a private life under article 8 or his right not to discriminated against under article 14. The court also rejected a challenge to the discretion exercised by the Chief Constable under section 64(1A) in relation to the retention of fingerprints and other samples.

VII. The appeal to the Court of Appeal

15 The shape of the case changed before the Court of Appeal. Liberty was given permission to intervene. In particular Liberty emphasised in para 3.4.3 of their intervention:

> "In contrast to fingerprints and DNA profiles, the physical *samples* which are retained and used under PACE (swabs, etc) and from which DNA is taken, potentially contain very much greater, more personal and detained information about an individual. This may include highly private matters such [as] information about a latent genetic illness, or the birth gender of a transsexual person. It may even reveal behavioural tendencies, or important information about the individual that he does not even know about himself such as the true nature of his familial relationships."

Liberty contended that "the range of genetic information that may be derived from DNA *samples* is of a highly private nature": para 1.3(1). In short Liberty argued that the samples provided more information about the person who provided the samples than is needed for the identification of those involved in crime. Faced with these new issues, which the Secretary

of State and the Chief Constable had no opportunity at the oral hearing to deal with, the Court of Appeal gave them leave to produce further evidence and to make further written submissions. That was done. The most important document placed before the Court of Appeal after the oral hearing was the affidavit of Dr Bramley to which some reference has already been made.

16 Addressing the issues, as amplified by Liberty's intervention, the Court of Appeal by a majority (Lord Woolf CJ and Waller LJ) upheld for somewhat different reasons the decision of the Divisional Court. In a dissenting judgment Sedley LJ concluded that the Chief Constable was required to consider whether in each particular case the individual concerned is free of any taint of suspicion.

VIII. The issues before the House

17 The agreed statement of facts and issues summarises the issues before the House as follows: (1) whether the retention of fingerprints, samples and DNA profiles is an interference with the appellants' right to respect for private life pursuant to article 8(1) of the Convention and, if so, whether it can be justified under article 8(2); (2) whether a distinction should be made between the retention of DNA profiles and samples; (3) whether the retention of the appellants' fingerprints, samples and DNA profiles amounts to discrimination against them for the purposes of article 14 of the Convention and, if so, whether it is objectively justified; (4) if the retention of fingerprints and DNA profiles and/or samples is an unjustified interference with the appellants' Convention rights, whether it would be possible to give section 64(1A) a Convention-compatible interpretation under section 3 of the 1998 Act; (5) if that is impossible, whether section 64(1A) should be declared to be incompatible with article 8 and/or 14 of the Convention; (6) whether the policy of the Chief Constable to retain samples and fingerprints in all cases subject to exceptional circumstances is unlawful and incompatible with the appellants' Convention rights. These issues must primarily be considered in the light of the coinpeting arguments of the parties. But the contentions of Liberty are also important. Although the Appellate Committee was willing to allow Liberty to intervene in writing and orally, that did not happen. The House has, however, considered in detail the written intervention of Liberty in the Court of Appeal as well as a petition by Liberty to the House of Lords to intervene which was subsequently withdrawn.

18 A procedural issue arose at the oral hearing of the appeals in the House. Counsel for the appellants applied for leave to introduce a letter dated 11 June 2004 from the Information Commissioner to Liberty about the National DNA Database as well as associated materials. The Information Commissioner is not a party to the proceedings and, although aware of the proceedings, did not seek leave to intervene. Not surprisingly, the Home Secretary and the Chief Constable strongly objected to the admission of this material. In my view this eleventh-hour attempt to introduce new material must be strongly deprecated and by itself this factor is sufficient reason to refuse the application. In the result the House looked at the material de bene esse. In my view the material does not assist in the disposal of the issues. I would reject the application.

IX. The legislative scheme

19 Before it will be possible to examine the issues directly it is necessary to explain the legislative scheme in some detail. Inherent in the PACE regime are three different concepts, viz the taking of fingerprints and samples, the retention of them, and the use of them.

Taking

20 The powers to take fingerprints and samples are to be found in PACE. Since fingerprints and samples were taken from the appellants in early 2001 those powers have in various respects been enlarged by statutory amendment but these changes are not material to the issues to be considered. PACE deals with fingerprints and samples separately. Sections 27 and 61 contain the main powers to take fingerprints in carefully regulated circumstances involving, amongst other things, a reasonable suspicion that a person has committed a criminal offence. The main power to take samples was to be found in section 63. It covers the case where a person was charged with a recordable offence.

21 It is true that the taking of fingerprints and samples involves an interference with the individual's private life within the meaning of article 8(1) of the Convention. On the other hand, such interference for the very limited statutory purposes is plainly objectively justified under article 8(2).

Retention

22 The terms of section 64(1A) of PACE have already been quoted. In order to place it in context, I set it out again:

> "Where—(a) fingerprints or samples are taken from a person in connection with the investigation of an offence, and (b) subsection (3) below does not require them to be destroyed, the fingerprints or samples may be retained after they have fulfilled the purposes for which they were taken but shall not be used by any person except for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution."

Section 64(1B) extends by definition the use for the purposes of section 64(1A) of checks of fingerprints and samples. It is also necessary to refer to the following subsections of section 64:

> "(3) If—(a) fingerprints or samples are taken from a person in connection with the investigation of an offence; and (b) that person is not suspected of having committed the offence, they must, except as provided in the following provisions of this section, be destroyed as soon as they have fulfilled the purpose for which they were taken.
>
> "(3AA) Samples and fingerprints are not required to be destroyed under subsection (3) above if—(a) they were taken for the purposes of the investigation of an offence of which a person has been convicted; and (b) a sample or, as the case may be, fingerprint was also taken from the convicted person for the purposes of that investigation.
>
> "(3AB) Subject to subsection (3AC) below, where a person is entitled under subsection (3) above to the destruction of any fingerprint or sample

taken from him (or would be but for subsection (3AA) above), neither the fingerprint nor the sample, nor any information derived from the sample, shall be used—(a) in evidence against the person who is or would be entitled to the destruction of that fingerprint or sample; or (b) for the purposes of the investigation of any offence; and subsection (1B) above applies for the purposes of this subsection as it applies for the purposes of subsection (1A) above.

"(3AC) Where a person from whom a fingerprint or sample has been taken consents in writing to its retention—(a) that sample need not be destroyed under subsection (3) above; (b) subsection (3AB) above shall not restrict the use that may be made of the fingerprint or sample or, in the case of a sample, of any information derived from it; and (c) that consent shall be treated as comprising a consent for the purposes of section 63A(1C) above; and a consent given for the purposes of this subsection shall not be capable of being withdrawn.

"(3AD) For the purposes of subsection (3AC) above it shall be immaterial whether the consent is given at, before or after the time when the entitlement to the destruction of the fingerprint or sample arises."

Subsection 63(3AC) is of particular interest in so far as it may have to be accommodated in the submissions on behalf of the appellants.

Use

23 Counsel for the Home Secretary accepted that it is possible to conceive of uses which might theoretically be capable of amounting to an interference with respect for private life under article 8(1). He gave the example that where samples were used to extract personal genetic information about an individual and that information was used in a way linked to that individual it might represent an interference with the right to respect for private life. Subject to such unusual cases, the use of retained fingerprints and samples in the context of the detection and prosecution of crime should cause no problem of principle.

24 Under this heading it is also important to bear in mind the decision of the House in *Attorney General's Reference (No 3 of 1999)* [2001] 2 AC 91. It was decided under the old section 64 and in respect of a sample which should undoubtedly have been destroyed. The House held that:

"whereas section 64(3B)(a) of [PACE] made express prohibition against the use in evidence of a DNA sample which should have been destroyed, section 64(3B)(b), in prohibiting the use of an unlawfully retained sample for the purposes of any investigation, did not amount to a mandatory exclusion of evidence obtained as a result of a failure to comply with that prohibition but, read with section 78 of [PACE], left the question of its admissibility to the discretion of the trial judge; that a decision by a judge in the exercise of his discretion to admit such evidence would not amount to an unlawful interference with the defendant's right to private life under article 8 of the Convention . . ."

The House was influenced by the broad policy consideration that, at p 118:

"respect for the privacy of defendants is not the only value at stake. The purpose of the criminal law is to permit everyone to go about their daily lives without fear of harm to person or property. And it is in the

A interests of everyone that serious crime should be effectively investigated and prosecuted. There must be fairness to all sides. In a criminal case this requires the court to consider a triangulation of interests. It involves taking into account the position of the accused, the victim and his or her family, and the public."

This approach may be of continuing relevance.

B

X. Issue (1): article 8

Does retention interfere with the right under article 8(1)?

25 There is no decision of the European Court of Human Rights on the question whether the retention of fingerprints or samples amounts to an interference with the right to respect for private life. On the other hand, the C European Commission of Human Rights has considered the point. In *McVeigh, O'Neill and Evans v United Kingdom* (1981) 5 EHRR 71, 103–104, paras 223–226 the Commission distinguished between the taking of fingerprints, photographs and records, and their retention. About retention the Commission stated, in para 227:

D "that it is open to question whether the retention of fingerprints, photographs and records of such information amounts to an interference with the applicants' right to respect for private life under article 8(1) of the Convention."

McVeigh's case involved charges of terrorism but the same reasoning may be applicable to other serious crimes. Subsequently, in the context of photographs and fingerprints retained in connection with a charge of fraud E the Commission concluded that there was not an interference with respect for private life under article 8: *Kinnunen v Finland* (Application No 24950/94) (unreported) 15 May 1996.

26 These decisions are relevant but far from conclusive. In the Divisional Court Leveson J, at para 21, was content simply to record that he was "far from convinced that the retention of photographs and F DNA samples engage article 8 in any form". A different approach prevailed in the Court of Appeal [2002] 1 WLR 3223. The court held that article 8(1) applied to the retention. Lord Woolf CJ found the solution in the different cultural traditions of member states. He said, at p 3233, para 32:

"So far as this jurisdiction is concerned it is my view that fingerprints and DNA samples are material which is regarded as being personal to the G individual from whom it is taken and so requires legal justification before it can be retained."

He explained, at p 3234, para 34:

"while not substantial, the interference is still real. There is no doubt a rainbow of reactions which are possible to intrusions of this nature, but at least for a substantial proportion of the public there is a strong objection H to the state storing information relating to an individual unless there is some objective justification for this happening. The objection to the storage is reflected in the appreciative public response to novels such as Aldous Huxley's *Brave New World* and George Orwell's *1984*. As to the persuasive decisions of the Commission, it has to be remembered that just

> as in the appropriate circumstances a margin of appreciation has to be extended for any shortcomings in this jurisdiction in relation to observing the Convention, so there can be situations where the standards of respect for the rights of the individual in this jurisdiction are higher than those required by the Convention. There is nothing in the Convention setting a ceiling on the level of respect which a jurisdiction is entitled to extend to personal rights. In this jurisdiction I would not expect a court to necessarily follow the decision of the Commission in *Reyntjens v Belgium* (1992) 73 DR 136, 152 that: 'The obligation to carry an identity card and to show it to the police whenever requested to do so does not as such constitute an interference in a person's private life within the meaning of article 8 of the Convention.' "

Waller LJ, at p 3240E, para 58, said that Liberty's intervention persuaded him that there was a breach of article 8(1) in the retention and use of the samples. Sedley LJ, at p 3243, para 68, agreed with the observations of Lord Woolf LJ on the application of article 8(1). He added that "we are fully entitled to take into account the strong cultural unease in the United Kingdom about the official collection and retention of information about individuals". Counsel for the appellants relied on these observations in the Court of Appeal. It is necessary to examine them.

27 While I would not wish to subscribe to all the generalisations in the Court of Appeal about cultural traditions in the United Kingdom, in comparison with other European states, I do accept that when one moves on to consider the question of objective justification under article 8(2) the cultural traditions in the United Kingdom are material. With great respect to Lord Woolf CJ the same is not true under article 8(1). Expressing the unanimous view of the House in *R (Ullah) v Special Adjudicator* [2004] 3 WLR 23, 39–40, para 20 Lord Bingham of Cornhill observed that the Convention is an international instrument, the correct interpretation of which can be authoritatively expounded only by the Strasbourg court. He added:

> "It is of course open to member states to provide for rights more generous than those guaranteed by the Convention, but such provision should not be the product of interpretation of the Convention by national courts, since the meaning of the Convention should be uniform throughout the states party to it. The duty of national courts is to keep pace with the Strasbourg jurisprudence as it evolves over time: no more, but certainly no less."

The question whether the retention of fingerprints and samples engages article 8(1) should receive a uniform interpretation throughout member states, unaffected by different cultural traditions. And the current Strasbourg view, as reflected in decisions of the Commission, ought to be taken into account.

28 That brings me to the concerns of Liberty. They centre on the retention of DNA samples. To the extent that Liberty expresses fears about the misuse of retained samples, Dr Bramley (paras 12.1–12.5) has shown the extent of the rigorous safeguards in place. In any event, the trial process ought to weed out such abuses. Liberty's fears of what may happen in the future in the light of the expanding frontiers of science is not relevant in

respect of contemporary use of retained samples in connection with the detection and prosecution of crime. If future scientific developments require it, judicial decisions can be made, when the need occurs, to ensure compatibility with the Convention.

29 In the Divisional Court Leveson J helpfully explained why the retention of DNA samples does not have an impact on the private lives of individuals. He said:

> "19. . . . A person can only be identified by fingerprint or DNA sample either by an expert or with the use of sophisticated equipment or both; in both cases, it is essential to have some sample with which to compare the retained data. Further, in the context of the storage of this type of information within records retained by the police, the material stored says nothing about the physical make-up, characteristics or life of the person to whom they belong."

Since the hearing in the Divisional Court, Dr Bramley has provided detailed and powerful support for this view. Dr Bramley explained that: (1) the scientific testing of the sample which leads to the generation of a DNA profile is based upon analysis of the non-coding region of DNA (namely STRs [short tandem repeats]): paras 3.2, 3.3 and 4.1; (2) the STR analysis performed to create a DNA profile does not generally permit extraction of potential medical information about an individual: para 4.2; (3) although other genetic information from samples could be obtained in theory (such as medical information), the use of samples obtained and retained under PACE is limited to purposes related to the prevention or detection of crime: para 11; (4) as explained by Dr Bramley (para 11.3):

> "The use to which the retained scrapes can be put is restricted by the legislation which permits their retention only for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution. This is not interpreted so widely as to allow general testing of the retained CJ scrapes for medical conditions or susceptibilities and linking the results to a specific known individual."

30 Counsel for the appellants then approached the matter from a different angle. He emphasised that the use of retained fingerprints and samples under section 64(1A) extends to "purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution". He argued that the words "for purposes related to" are capable of permitting uses other than for the investigation, detection or prosecution of crime. The text shows that the words "for purposes relating to" apply to each of the three specified uses, i e (a) for purposes related to the prevention or detection of crime; (b) for purposes related to the investigation of an offence; (c) for purposes related to the conduct of a prosecution. And the context shows that the words "for purposes related to" fulfil a meaningful role. These words permit use of fingerprints and samples for *exculpation* of a potential suspect, or use of fingerprints and samples on a criminal appeal or for investigation of a miscarriage of justice. Such permitted uses might otherwise be said to have been excluded if a very restrictive definition of "conduct of prosecution" or "investigation of an offence" were to be adopted. In these circumstances, and bearing in mind the interpretive obligation in section 3 of the 1998 Act, the fears of counsel

for the appellants are not justified. In so far as it may be necessary section 64(1A) will be given a Convention-compatible meaning under section 3 of the 1998 Act.

31 Looking at the matter in the round I incline to the view that in respect of retained fingerprints and samples article 8(1) is not engaged. If I am wrong in this view, I would say any interference is very modest indeed.

If the retention of DNA profiles, samples and fingerprints is a breach of article 8(1), is it justified under article 8(2)?

32 This issue does not arise if the conclusion is correct that article 8(1) is not engaged. I will consider it, however, on the hypothesis that there is some interference with private life, albeit rather modest.

33 The effect of the decision of the House in *Attorney General's Reference (No 3 of 1999)* [2001] 2 AC 91, in conjunction with section 64 of PACE in unamended form, left the law in a distinctly unsatisfactory state. There was an obligation to destroy fingerprints and samples in respect of persons who were acquitted. Nevertheless, if such material was unlawfully retained, it could be used for the purpose of investigating another offence, and the evidence could be used in a subsequent trial unless it was excluded at the judge's discretion. This distinction did not reflect well on the law. Parliament could have reversed *Attorney General's Reference (No 3 of 1999)*. Instead, adopting the underlying philosophy of the House in that decision, Parliament decided to provide for the retention of fingerprints and samples. This legislative choice must be approached with due deference to a policy decision made by Parliament.

34 The appellants argued that an interference with article 8(1) cannot be justified under article 8(2). The Divisional Court dismissed this argument. The Court of Appeal unanimously rejected an appeal on this part of the case.

35 In the House counsel for the appellants renewed the submissions (1) that retention is not "in accordance with law"; and (2) that the power of retention is disproportionate.

36 The first contention can be dealt with briefly. Counsel cited *Silver v United Kingdom* (1983) 5 EHRR 347, 372, para 88 for the proposition that "a law which confers a decision must indicate the scope of that discretion". Standing alone this is an impractical and unworkable prescription. But the European Court of Human Rights added:

> "the court has already recognised the impossibility of attaining absolute certainty in the framing of laws and the risk that the search for certainty may entail excessive rigidity . . . the court points out once more that 'many laws are inevitably couched in terms which, to a greater or lesser extent, are vague and whose interpretation and application are questions of practice."

The discretion involved in the power to retain fingerprints and samples makes allowance for exceptional circumstances, e g where an undertaking to destroy the fingerprints or sample was given or where they should not have been taken in the first place, as revealed by subsequent malicious prosecution proceedings. Sometimes an obviously unmeritorious point does not require elaborate examination. In agreement with his colleagues Sedley LJ [2002] 1 WLR 3223, 3243, para 69 dealt with the argument as follows:

A "The next question is whether retention of fingerprints or of bodily samples which is permitted under section 64 of PACE is justified under article 8(2). The purposes of retention—the prevention of crime and the protection of the right of others to be free from crime—are four-square within article (8(2), and retention is provided for by law."

I respectfully agree.

B 37 The second contention is based on the principle of proportionality. Counsel for the appellants argued that the retention of fingerprints and DNA samples creates suspicion in respect of persons who have been acquitted. Counsel for the Home Secretary said that this argument focuses on the wrong target. The retention of fingerprints and DNA samples is not aimed at the past. Its purpose is to assist in the investigation of offences in the future. The retention and use of fingerprints and samples in this way C does not affect the appellants unless they are implicated in a future crime, by a DNA sample found at the scene. It is only if and when there are two profiles which match each other that the database will generate a bull's eye.

38 The following propositions seem to be established: (i) the fingerprints and samples are kept only for the limited purpose of the detection, investigation, and prosecution of crime; (ii) the fingerprints and D samples are not of any use without a comparator fingerprint or sample from the crime scene; (iii) the fingerprints and samples will not be made public; (iv) a person is not identifiable to the untutored eye simply from the profile on the database, any interference represented by the retention being minimal; (v) and, on the other hand, the resultant expansion of the database by the retention confers enormous advantages in the fight against serious E crime. Cumulatively these factors suggest that the retention of fingerprints and samples is not disproportionate in effect.

39 Counsel for the appellants submitted that the legislative aim could be achieved by less intrusive means. It became clear that this contention would require a case-by-case consideration of the circumstances of alleged offences of which the individual has been acquitted. Counsel was able to rely on the conclusion of Sedley LJ. He said, at p 3249, para 94:

F "The power of a Chief Constable to destroy data which he would ordinarily retain must in my judgment be exercised in every case, however rare such cases may be, where he or she is satisfied on conscientious consideration that the individual is free of any taint of suspicion."

In my view this would not confer the benefits of a greatly extended database and would involve the police in interminable and invidious disputes (subject G to judicial review of individual decisions) about offences of which the individual had been acquitted. In any event, Waller LJ pointed out, at pp 3242–3243, para 66:

"to introduce a concept of a Chief Constable having to consider whether a person is free of any taint of suspicion has great difficulties, and as it seems to me is raising a consideration which in fact should not apply H at the retention stage. At the retention stage consideration of the circumstances of the *offence* of which the person has by this stage been acquitted seems to me almost certainly irrelevant. I accept that if some form of undertaking were given to destroy to induce a person to co-operate in the taking of a sample, that would be relevant, but the

circumstances of the offence itself would as I see it not be. Apart from the 'undertaking type case', retention is only relevant to the question whether the details on the databank will assist in either the elimination or the conviction of a person so far as some future criminal investigation is concerned. If justification for retention is in any degree to be by reference to the view of the police on the degree of innocence, then persons who have been acquitted and have their samples retained can justifiably say this stigmatises or discriminates against me—I am part of a pool of acquitted persons presumed to be innocent, but I am being treated as though I was not. It is not in fact in any way stigmatising someone who has been acquitted to say simply that samples lawfully obtained are retained as the norm, and it is in the public interest in its fight against crime for the police to have as large a database as possible. I accordingly do not subscribe to the view that the Chief Constable is bound to exercise his discretion in the way suggested by Sedley LJ."

These observations were made in the context of the issue of discretion but are apposite to the question whether there are less intrusive but realistic means available to achieve the legislative purpose. In my view the answer is that there are not.

40 I would, therefore, hold that if article 8(1) is engaged, there is plainly an objective justification under article 8(2).

XI. Issue (2): Distinction between the retention of DNA profiles and samples.

41 It will be apparent from my examination and discussion of the undoubted distinction between DNA profiles and samples (ante, para 5) that, for the reasons already given, the legal consequences are not as contended for by counsel for the appellants and Liberty. It is unnecessary to traverse the same ground again.

XII. Issue (3): Does the retention of fingerprints and samples amount to discrimination under article 14 and, if so, can it be objectively justified?

42 Based on the approach of Brooke LJ in *Wandsworth London Borough Council v Michalak* [2003] 1 WLR 617; 625, para 20, as amplified in *R (Carson) v Secretary of State for Work and Pensions* [2002] EWHC 978 (Admin), para 52; [2003] 3 All ER 577, five questions can be posed as a framework for considering the question of discrimination. (1) Do the facts fall within the ambit of one or more of the Convention rights? (2) Was there a difference in treatment in respect of that right between the complainant and others put forward for comparison? (3) If so, was the difference in treatment on one or more of the proscribed grounds under article 14? (4) Were those others in an analogous situation? (5) Was the difference in treatment objectively justifiable in the sense that it had a legitimate aim and bore a reasonable relationship of proportionality to that aim?

43 But a caveat must be mentioned. In *Ghaidan v Godin-Mendoza* [2004] 3 WLR 113, 157, para 134, Baroness Hale of Richmond explained:

"the *Michalak* questions are a useful tool of analysis but there is a considerable overlap between them: in particular between whether the situations to be compared were truly analogous, whether the difference in

A treatment was based on a proscribed ground and whether it had an objective justification. If the situations were not truly analogous it may be easier to conclude that the difference was based on something other than a proscribed ground. The reasons why their situations are analogous but their treatment different will be relevant to whether the treatment is objectively justified. A rigidly formulaic approach is to be avoided."

B That is how I will approach the matter.

Question 1: a Convention right

44 There is no free-standing right under article 14 against discrimination. In this case the question is whether the facts fall within the ambit of article 8. If my conclusion is right that article 8(1) is not engaged, it C follows that article 14 is not triggered. I will assume, however, that the retention of fingerprints and samples does amount to an interference under article 8(1), albeit a justified interference under article 8(2). On this supposition the first *Michalak* question must be answered in the affirmative.

Question 2: less favourable treatment

D 45 The appellants' chosen comparators are the general body of persons who have not had fingerprints and samples taken by the police in the course of a criminal investigation. There is different treatment between those comparators and the appellants in relation to section 64(1A) of PACE.

Question 3: a proscribed ground?

E 46 This question is important because if the different treatment is not on a relevant ground for the purposes of article 14, then this article is not applicable. In any event, identification of the ground for different treatment is material to the question of justification.

47 The different treatment afforded to the appellants and comparators was on the ground that the former had already provided samples and fingerprints to the police in a criminal investigation while the comparators F had never been required to do so.

48 The list of grounds in article 14 is not exhaustive, and necessarily includes each of the specifically proscribed grounds as well as "other status". The European Court of Human Rights has interpreted "other status" as meaning a personal characteristic: *Kjeldsen, Busk Madsen and Pedersen v Denmark* (1976) 1 EHRR 711, 732–733, para 56. I do not understand Lord G Woolf CJ [2002] 1 WLR 3223, 3238 to have expressed a different view in paragraph 47 of his judgment. On the other hand, the proscribed grounds in article 14 cannot be unlimited, otherwise the wording of article 14 referring to "other status" beyond the well-established proscribed grounds, including things such as sex, race or colour, would be unnecessary. It would then preclude discrimination on any ground. That is plainly not the meaning of article 14.

H 49 It is, therefore, necessary to examine whether the ground for different treatment in this case amounts to a status in the sense of a personal characteristic within the meaning of article 14.

50 There is a difference in treatment between those who have had to provide fingerprints and samples pursuant to a criminal investigation as

compared with the rest of the public who have not. But that difference is not necessarily on grounds of "status". Counsel for the Chief Constable and counsel for the Home Secretary submitted that it is a difference simply reflecting historical fact, namely that the authorities already hold the fingerprints and samples of the individuals concerned which were lawfully taken. Counsel for the Chief Constable illustrated the point with an analogy. He asked the House to imagine that Mr Marper had been involved in an accident and admitted to hospital. In routine fashion notes would have been made, tests done and X-rays taken. A subsequent request by his solicitors to destroy the materials would have been refused by the hospital. First, it is good practice to keep them. Secondly, medical negligence is a growing area of litigation and prudence requires records to be kept. Had Mr Marper then sought a judicial review of this decision, an article 8 challenge would have failed and an article 14 challenge would have met the answer that the existence of the records is not a matter of status. It is an historical fact that is unrelated to any personal characteristic. I find the analogy, and the argument which it supports, persuasive. This is, however, not the only possible explanation. In the Court of Appeal Sedley LJ observed, at p 3247, para 86:

> "The line between those unconvicted people who have faced charges and those who have not, while not a bright line, is not arbitrarily drawn. It does not tarnish the innocence of the unconvicted in the eye of the law. But it recognises that among them is an indeterminate number who are likelier than the rest of the unconvicted population to offend in the future or to be found to have offended in the past."

This view was adopted by counsel on behalf of the Chief Constable but not by counsel on behalf of the Home Secretary. Given my acceptance of the rationale put forward jointly by the Chief Constable and the Home Secretary it is not necessary to rule on the observation of Sedley LJ.

51 By way of summary the position is as follows. The difference in treatment is not analogous to any of the expressly proscribed grounds such as sex, race, gender or religion. The fact that the police are now in possession of fingerprints and samples which were previously lawfully acquired as a result of a criminal investigation does not give rise to a "status" within the meaning of article 14. The appellants, and other individuals in their position, are as fully entitled to the presumption of innocence as the general body of citizens.

52 I would accept the analysis of counsel that the difference in treatment of the appellants and those who have not been investigated and provided fingerprints is not a proscribed ground under article 14.

Question 4: analogous situation?

53 For reasons already given there is a material distinction between individuals who have had their fingerprints and samples lawfully taken in consequence of being charged with a recordable offence and those who have not. It cannot be said that the circumstances are so similar as to call for a positive justification of the difference in treatment. I have taken into account the analogy of indirect discrimination advanced by Sedley LJ, at pp 3247–3248, paras 89–92. In my view we are dealing with an allegation of direct discrimination apparent on the face of the legislation. The analogy is not

A apposite. Within the *Michalak* framework (*Wandsworth London Borough Council v Michalak* [2003] 1 WLR 617) the pool of comparators has been wrongfully identified by the appellants. It follows that I would answer the question by concluding that the appellants and the suggested comparators are not in an analogous situation.

B *Question 5: objective justification*

54 If, contrary to my view, it is necessary to consider the justification for the difference in treatment, I would conclude without hesitation that objective justification is established. First, the element of legitimate aim is plainly present inasmuch as the increase in the database of fingerprints and samples promotes the public interest by the detection and prosecution of serious crime and by exculpating the innocent. This conclusion is
C powerfully reinforced by the recent statistics which I have cited in paragraph 8 of this opinion.

55 Secondly, in my view, the requirement of proportionality is satisfied. Section 64(1A) of PACE objectively represents a measured and proportionate response to the legislative aim of dealing with serious crime. Moreover, this conclusion is supported by the need, in the circumstances, to
D approach with due deference the policy decision made by Parliament in enacting section 64(1A) in the fight against serious crime. And the results of the new scheme provide cogent vindication of the decision of Parliament.

Conclusion on article 14

56 I would hold that there is no breach of article 14.

E *XIII. Issues (4) and (5)*

57 Given these conclusions, issue 4 (interpretation under section 3 of the 1998 Act) and issue 5 (incompatibility under section 4 of the 1998 Act) fall away.

XIV. Issue (6): Discretion

F

58 The nature of the policy adopted by the Chief Constable of the South Yorkshire Police and other Chief Constables is plain. It is to retain, save in exceptional cases, all fingerprints and samples taken from those who have been acquitted of criminal offences or against whom proceedings have not been pursued. The aim of the policy is directed to the prevention or detection of crime, the investigation of offences, the facilitation of
G prosecutions, and the speedy exculpation of the innocent as well as the correction of miscarriages of justice.

59 Counsel for the appellants argued that this "blanket policy" is unlawful. He submitted that the policy is a fetter on the discretion of the Chief Constable. He said that retaining fingerprints in the case of persons untainted by suspicion is disproportionate. Counsel argued that the only fair solution is a case-by-case examination of the circumstances of each case.
H That, of course, would mean an examination of the circumstances which led to the fingerprints and samples being taken in respect of the alleged offence of which the individual was subsequently cleared. He accepted that this would involve the examination of many thousands of cases and involve large numbers of decisionmakers.

60 As I pointed out in para 39 of this opinion such a system would probably not confer the benefits of a greatly extended database and would involve the police in interminable and invidious disputes (with individual decisions subject to judicial review) about the circumstances of offences of which individuals had been cleared. Moreover, in such a decision-making process individuals who are not eliminated as being without a taint of suspicion could truly complain that they have been deprived of the benefit of the presumption of innocence. This suggested alternative is unrealistic and impractical.

61 I would, therefore, reject the challenge to the policy. It is lawful.

XV. Disposal

62 I would dismiss the appeals.

LORD RODGER OF EARLSFERRY

63 My Lords, I have had the advantage of reading the speech of my noble and learned friend, Lord Steyn, in draft. I agree with it and, for the reasons he gives, I too would dismiss the appeals.

64 In particular, it respectfully appears to me that the Court of Appeal attached too much weight to what they saw as a greater cultural resistance in Britain than in other European countries to the collection and retention of data about individuals. For one thing, I am doubtful whether the reaction of the educated public at the time to novels published many years ago can be taken as an accurate reflection of British public opinion in the very different conditions of today. Recent press reaction to the failure of police and other bodies to store information about those suspected of sexual offences might well point to a rather different attitude. And it may well be that, with their bitter experience of life under totalitarian regimes, people in some other European countries would nowadays be more concerned than people here about official files on individuals.

65 In any event the attitude in Britain alone cannot be decisive. At most, it would be a basis on which Parliament might have chosen to enact legislation to prevent the storing of information about suspects or on which the courts might have developed the common law so as to provide such protection. But, in fact, by enacting section 82 of the Criminal Justice and Police Act 2001, Parliament has removed the provision which previously made it unlawful to retain the fingerprints and samples of those who were subsequently not charged or who were acquitted. And that must be regarded as the most recent expression of public policy on this topic in England and Wales. (In Scotland no such change has been made so far.)

66 In these circumstances the appellants seek to rely on the article 8(1) Convention right which they enjoy under the Human Rights Act 1998. That is a right under domestic law, but a right of a special kind which was, in the words of Lord Nicholls of Birkenhead in *In re McKerr* [2004] 1 WLR 807, 815E, para 25, "created by the 1998 Act by reference to the Convention". So, in order to interpret article 8 and the other Convention rights in Schedule 1 to the 1998 Act, courts must have regard to the scope of the equivalent rights in the Convention. For that reason, while the decisions of the European Court of Human Rights on the interpretation of the Convention are not binding, they provide authoritative guidance which courts have to take into account when interpreting the rights in domestic

A law. In formulating its decisions the court considers the spectrum of attitudes across the contracting states in order to determine the contemporary content of rights under the Convention. It is the decisions reached in this way that help to shape the content of the Convention rights in our domestic law. I refer to the observations of Lord Bingham of Cornhill in *R (Ullah) v Special Adjudicator* [2004] 3 WLR 23, 39–40, para 20. So far at
B least, as Lord Steyn has shown, the Strasbourg case law does not support the appellants' argument that there has been a violation of article 8 in the circumstances of these cases.

BARONESS HALE OF RICHMOND

67 My Lords, sadly, while I agree with everything else in the opinion of my noble and learned friend, Lord Steyn, I cannot agree with the view, to
C which he is inclined, that the retention and storage of fingerprints, DNA profiles and samples is not an interference with the appellants' rights under article 8(1).

68 I agree that it is necessary to distinguish between the taking of fingerprints and samples, the deriving of information from those samples, the storage of samples and information, and the use of either samples or
D information for some particular purpose. The justifications for each of these may be very different. But all of them, in my view, constitute an interference by the state in a person's right to respect for his private life. This is an aspect of what has been called informational privacy. "This notion of privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit": per La Forest J in *R v Dyment* [1988] 2 SCR 417, 429.

E 69 In the powerful words of the Canadian Privacy Commissioner in his report on *Genetic Testing and Privacy* (1995), p 2 ("Introduction"):

> "The measure of our privacy is the degree of control we exercise over what others know about us. No one, of course, has absolute control. As social animals, few would want total privacy. However, we are all
F entitled to expect enough control over what is known about us to live with dignity and to be free to experience our individuality. Our fundamental rights and freedoms—of thought, belief, expression and association—depend in part on a meaningful measure of individual privacy. Unless we each retain the power to decide who should know our political allegiances, our sexual preferences, our confidences, our fears and aspirations, then the very basis of a civilised, free and democratic
G society could be undermined."

70 It could be said that the samples are not "information": see, for example, the doubts expressed about this by the Australian Law Reform Commission in Essentially Yours: The Protection of Human Genetic Information in Australia, ALRC 96, para 8.8. But the only reason that they are taken or kept is for the information which they contain. They are not
H kept for their intrinsic value as mouth swabs, hairs or whatever. They are kept because they contain the individual's unique genetic code within them. They are kept as information about that person and nothing else. Fingerprints and profiles are undoubtedly information. The same privacy principles should apply to all three.

71 It can also be said that not all information about a person is so private that it enjoys the protection of article 8. This is so. There must be a reasonable expectation of privacy before it is protected: see *Campbell v MGN Ltd* [2004] 2 WLR 1232. But there can be little, if anything, more private to the individual than the knowledge of his genetic make-up. Again in the words of the Canadian Privacy Commissioner: "No surveillance technology is more threatening to privacy than that designed to unlock the information contained in human genes."

72 Hence it is common ground that the *taking* of fingerprints and DNA samples is an interference with the article 8(1) right, even though the invasion of bodily integrity involved is minimal. It is also common ground that the *use* of the information derived from them is such an interference. This must be because the information is regarded as intrinsically private.

73 If the taking and use of the information is an interference, it is difficult to see why the retention, storage or keeping of that information is not also an interference. Storing information almost inevitably involves someone else knowing it. It is an interference with privacy for someone to know or have access to private information even if they make no other use of it. The mere fact that someone has read my private correspondence or seen my bank accounts is an interference with my privacy even if that person tells no one else what he has seen. That is why access to private information such as that contained in medical records has to be carefully controlled. The fact that only a few people can understand the information does not affect the principle, although it may affect the justification.

74 Nor can it be irrelevant that storing this information is a necessary prelude to using it. Some uses, in particular those for which the information in this case is permitted to be used, are entirely justifiable and beneficial. But others may not be. To return to the Canadian Privacy Commissioner:

> "Modern explorers have set sail on voyages into the genetic microcosm, seeking a medically powerful but potentially dangerous treasure: information about how our genes make us tick. Today, we can ask who among us is likely to have healthy babies or fall ill with a genetic disease. In the future, we may be able to use genetic testing to tell us who will be smart, be antisocial, work hard, be athletic or conform to prevailing standards of beauty."

75 No one is thinking of using the samples collected here for such purposes. But the fact that they could be so used, perhaps many years in the future, means that the appellants have a very real interest in how they are stored and who has access to them while they are stored. I do not believe that this interest is peculiar to the cultural traditions of this country. There is ample evidence of concern about them elsewhere in the world. Our data protection laws were originally the product of a Council of Europe Convention in 1981.

76 The general tenor of the jurisprudence of the European Court and Commission of Human Rights is that the retention, keeping or storage of private information by state institutions is an interference with article 8(1) rights. In *Leander v Sweden* (1987) 9 EHRR 433, 450, para 48 the European Court held that both the storage of private information in a secret police register and its release, coupled with a refusal to allow an opportunity to refute it, were an interference with the right to respect for private life. In

Friedl v Austria (1995) 21 EHRR 83, 88–89, paras 48–53 the Commission distinguished between the taking and keeping of photographs without identifying the subjects, and police questioning in order to establish identity and the recording of these personal data; the former was not an interference with article 8(1) but the latter was, although it was "relatively slight": p 91, para 66. The Commission reached a different conclusion about photographs and fingerprints kept after the applicant's acquittal in *Kinnunen v Finland* (Application No 24950/94) 15 May 1996; but they noted that the information had been properly taken on his arrest, did not contain any surveillance or similar information or opinions which he might wish to refute, and therefore "was not of such a character that it could have adversely affected the applicant any more significantly than the publicly known fact that he had been charged with, but acquitted of, certain charges". The Commission was therefore concentrating on the nature of the information and the ways in which it could adversely affect the applicant. Even then it may have been somewhat optimistic. But this case is not limited to fingerprints. For the reasons given earlier, the DNA information in this case is of a very different 'character' even if the present uses to which it can lawfully be put are the same.

77 If keeping and storing this information by the state were not an interference with the right guaranteed by article 8(1), the consequences would be surprising. First, it would not be necessary to find any justification for it under article 8(2). Of course, mere keeping of the information is a lesser interference than using it, and may be easier to justify. But it would be surprising if the state were free to do this without demonstrating a legitimate aim and that it was necessary to keep the information in this way in pursuit of that aim. Secondly, if article 8(1) is not engaged by the mere keeping of private information, then the state might be free to be thoroughly discriminatory in choosing which information to keep, without contravening article 14. It would be surprising if a decision to keep all the information obtained from, say, black suspects but not from whites did not contravene article 14. But unless the keeping falls within the ambit of article 8 it would not do so.

78 I accept that we must interpret the Convention rights in a way which keeps pace with rather than leaps ahead of the Strasbourg jurisprudence as it evolves over time. But it would be surprising if Strasbourg were not to consider it incumbent upon the state to justify its retention and storage of all this information but particularly the DNA samples and profiles. For the reasons given by my noble and learned friends, Lord Steyn and Lord Brown of Eaton-under-Heywood, I agree that this is readily done. The whole community, as well as the individuals whose samples are collected, benefits from there being as large a database as it is possible to have. The present system is designed to allow the collection of as many samples as possible and to retain as much as possible of what it has. The benefit to the aims of accurate and efficient law enforcement is thereby enhanced.

79 I therefore agree that these appeals should be dismissed.

LORD CARSWELL

80 My Lords, I have had the advantage of reading in draft the opinion prepared by my noble and learned friend Lord Steyn, and I fully agree with his reasons and his conclusions. I only wish to add a short comment about

one aspect of the judgments in the Court of Appeal which requires mention, since I feel that it might be misunderstood and applied incorrectly in future cases.

81 Sedley LJ [2002] 1 WLR 3223, 3247–3248, paras 88, 89, addressed the issue of selecting the pool of comparators in determining whether there had been discrimination. He expressed the view that the approach of the other members of the Court of Appeal to identifying the pool overlooked the importance of the principles to be applied in deciding if there had been indirect discrimination. He went on, at p 3248:

> "90. Central to indirect discrimination is the ostensibly neutral factor which on analysis significantly and unjustifiably disadvantages a protected group. *Griggs v Duke Power Co* (1971) 401 US 424 provides a well known example: because of educational disadvantage, black workers did significantly worse than white workers in literacy tests which were applied to all employees but were objectively unnecessary. The discriminating factor was not facing the literacy test but failing it. But its differential impact could only be measured in a pool consisting of both white and black workers—that is, both those disadvantaged and those not disadvantaged by it. In the present appeals the discriminating factor is not the fact of having had samples lawfully taken; it is being a person who has had them taken but has not then been convicted. To confine the pool for testing its effect to other people in the identical position, as Waller LJ would do, and to conclude—inexorably—that they are all being treated alike, is the equivalent of confining the pool in the *Griggs* case to black workers. The correct pool in such a case (that is, the pool which will test the particular complaint) is everybody in the same relevant situation: in the *Griggs* case, all the company's workers to whom the test was given; in the present appeals, all citizens who have not been convicted of an offence.
>
> 91. To take as your pool simply the group which asserts that it is being discriminated against and to find—as you practically always will—that they are all being treated the same is to defeat the rationale of indirect discrimination. To take as your pool a larger group which does not share the *relevant* characteristic—here, for example, *everyone* who has had their fingerprints and bodily samples lawfully taken—will be to sidestep the legal issue. The legal issue is not (as in another system it might have been) the absence of discrimination between convicted and acquitted suspects: it is the presence of discrimination between legally innocent people who respectively have and have not been investigated."

82 The logic of the reasoning adopted by Sedley LJ is valid in cases of indirect discrimination. In such cases, as he points out, it is necessary to include in the pool both those disadvantaged by the ostensibly neutral factor and those not so disadvantaged. If both classes are not included, then the ostensibly neutral factor which operates differently in respect of each group cannot operate to demonstrate the existence of a difference in result which amounts to discrimination. As Sedley LJ said, to do so defeats the rationale of indirect discrimination.

83 The reasoning must, however, be confined to cases of indirect discrimination. In those of direct discrimination the comparison is simply one of comparing the situation of the complainant, and possibly others in

like case, with other people in a comparable situation. The imperative created by the need to consider the ostensibly neutral factor does not apply in such a case. The present cases should in my opinion be classed as claims in respect of direct discrimination, for there is no ostensibly neutral factor which turns an apparent equality of treatment into an inequality. The identification of the group making up the pool and the comparison of the situation of each appellant and other persons in like case with that of the other members of the pool is more straightforward. I do not agree that the comparison should be between legally innocent people who respectively have and have not been investigated, as Sedley LJ suggests. Rather I consider, in agreement with Waller LJ, that the relevant pool consists of those persons from whom samples have been lawfully taken. Neither of the appellants was treated any differently from the other persons in that pool and accordingly there is no breach of article 14 of the Convention.

84 I agree that the appeals should be dismissed.

LORD BROWN OF EATON-UNDER-HEYWOOD

85 I have had the advantage of reading in draft the speech of my noble and learned friend Lord Steyn. I agree with all that he says on each of the issues raised and I wish to add only a few short paragraphs of my own. My concern is simply to indicate how very clear a case this seems to me to be. Indeed my only real problem now, following full investigation of the case with the assistance not only of the parties but from Liberty too, is in discerning any coherent basis on which the challenge can still be sustained.

86 Given the carefully defined and limited use to which the DNA database is permitted to be put—essentially the detection and prosecution of crime—I find it difficult to understand why anyone should object to the retention of their profile (and sample) on the database once it has lawfully been placed there. The only logical basis I can think of for such an objection is that it will serve to increase the risk of the person's detection in the event of his offending in future. But that could hardly be a legitimate objection, nor, indeed, is it advanced as such. Such objections as *were* suggested, however, seem to be entirely chimerical. First, the fear of an Orwellian future in which retained samples will be re-analysed by a mischievous state in the light of scientific advances and the results improperly used against the person's interest. If, of course, this were a valid objection it would apply no less to samples taken from the convicted as from the unconvicted and logically, therefore, it would involve the destruction of everyone's samples. But no such abuse is presently threatened and if and when it comes to be then will be the time to address it. Sufficient unto the day is the evil thereof.

87 The second suggested objection is to the retention of profiles obtained from those at one time reasonably suspected of crime but subsequently acquitted or not proceeded against, the objection being that they are thereby stigmatised as properly belonging to the same group as the convicted. This to my mind is an equally unrealistic objection. Mr Gordon was quite unable to suggest in whose eyes they would be stigmatised. It should not be forgotten that the profiles of pure volunteers (those falling within section 64(3AC) of PACE) are also retained on the database.

88 In short, it seems to me that the benefits of the larger database brought about by the now impugned amendment to PACE (as described in

Lord Steyn's judgment) are so manifest and the objections to it so threadbare that the cause of human rights generally (including the better protection of society against the scourge of crime which dreadfully afflicts the lives of so many of its victims) would inevitably be better served by the database's expansion than by its proposed contraction. The more complete the database, the better the chance of detecting criminals, both those guilty of crimes past and those whose crimes are yet to be committed. The better chance too of deterring from future crime those whose profiles are already on the database. And these, of course, are not the only benefits. The larger the database, the less call there will be to round up the usual suspects. Instead, those amongst the usual suspects who are innocent will at once be exonerated. Were these appellants to succeed in their challenge, the cause of justice would be seriously impeded.

89 I too would dismiss these appeals.

Appeals dismissed with costs.

Solicitors: Howells, Sheffield; Treasury Solicitor; Legal Services Department, South Yorkshire Police.

M G

116

CONSEIL DE L'EUROPE
COUNCIL OF EUROPE

COUR EUROPÉENNE DES DROITS DE L'HOMME
EUROPEAN COURT OF HUMAN RIGHTS

FOURTH SECTION

CASE OF LIBERTY AND OTHERS
v. THE UNITED KINGDOM

(Application no. 58243/00)

JUDGMENT

STRASBOURG

1 July 2008

FINAL

01/10/2008

This judgment will become final in the circumstances set out in Article 44 § 2 of the Convention. It may be subject to editorial revision.

117

In the case of Liberty and Others v. the United Kingdom,

The European Court of Human Rights (Fourth Section), sitting as a Chamber composed of:

Lech Garlicki, *President,*
Nicolas Bratza,
Ljiljana Mijović,
David Thór Björgvinsson,
Ján Šikuta,
Päivi Hirvelä,
Mihai Poalelungi, *judges,*
and Lawrence Early, *Section Registrar,*

Having deliberated in private on 10 June 2008,

Delivers the following judgment, which was adopted on that date:

PROCEDURE

1. The case originated in an application (no. 58243/00) against the United Kingdom of Great Britain and Northern Ireland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by Liberty, British Irish Rights Watch and the Irish Council for Civil Liberties, a British and two Irish civil liberties' organisations based in London and Dublin respectively, on 9 September 1999.

2. The applicants were represented by Mr A. Gask, a lawyer practising in London. The United Kingdom Government ("the Government") were represented by their Agent, Mr D. Walton, Foreign and Commonwealth Office.

3. On 25 June 2002 the Court decided to communicate the application to the Government, and several rounds of observations were received from the parties. On 22 March 2005 the Court adjourned the case until linked proceedings before the Investigatory Powers Tribunal had concluded (see paragraphs 11-15 below). On 27 February 2006 the Court resumed its examination and, under the provisions of Article 29 § 3 of the Convention, decided to examine the merits of the application at the same time as its admissibility. Further observations were, therefore, sought from the parties.

4. The applicants requested a hearing but the Court decided that it would not be necessary.

THE FACTS

THE CIRCUMSTANCES OF THE CASE

1. The alleged interception of communications

5. The applicants alleged that in the 1990s the Ministry of Defence operated an Electronic Test Facility ("ETF") at Capenhurst, Cheshire, which was built to intercept 10,000 simultaneous telephone channels coming from Dublin to London and on to the continent. Between 1990 and 1997 the applicants claimed that the ETF intercepted all public telecommunications, including telephone, facsimile and e-mail communications, carried on microwave radio between the two British Telecom's radio stations (at Clwyd and Chester), a link which also carried much of Ireland's telecommunications traffic. During this period the applicant organisations were in regular telephone contact with each other and also providing, *inter alia,* legal advice to those who sought their assistance. They alleged that many of their communications would have passed between the British Telecom radio stations referred to above and would thus have been intercepted by the ETF.

2. Complaint to the Interception of Communications Tribunal ("ICT")

6. On 9 September 1999, having seen a television report on the alleged activities of the ETF, the applicant organisations requested the Interception of Communications Tribunal ("the ICT": see paragraphs 28-30 below) to investigate the lawfulness of any warrants which had been issued in respect of the applicants' communications between England and Wales and Ireland. On 19 October 1999 an official of the ICT confirmed that an investigation would proceed and added:

> "... I am directed to advise you that the Tribunal has no way of knowing in advance of an investigation whether a warrant exists in any given case. The Tribunal investigates all complaints in accordance with section 7 of the [Interception of Communications Act 1985: 'the 1985 Act', see paragraphs 16-33 below] establishing whether a relevant warrant or relevant certificate exists or had existed and, if so, whether there has been any contravention of sections 2 to 5. If ... the Tribunal concludes that there has been a contravention of sections 2 to 5, the Tribunal may take steps under sections 7(4), (5) and (6). In any case where there is found to have been no contravention, the Tribunal is not empowered to disclose whether or not authorised interception has taken place. In such instances, complainants are advised only that there has been no contravention of sections 2 to 5 in relation to a relevant warrant or a relevant certificate."

7. By a letter dated 16 December 1999 the ICT confirmed that it had thoroughly investigated the matter and was satisfied that there had been no

contravention of sections 2 to 5 of the 1985 Act in relation to the relevant warrant or certificate.

3. Complaint to the Director of Public Prosecutions ("DPP")

8. By a letter dated 9 September the applicants complained to the DPP of an unlawful interception, requesting the prosecution of those responsible. The DPP passed the matter to the Metropolitan Police for investigation. By a letter dated 7 October 1999 the police explained that no investigation could be completed until the ICT had investigated and that a police investigation might then follow if it could be shown that an unwarranted interception had taken place or if any of the other conditions set out in section 1(2)-(4) of the 1985 Act had not been met. The applicants pointed out, in their letter of 12 October 1999, that the vague, albeit statutory, response of the ICT would mean that they would not know whether a warrant had been issued or, if it had, whether it had been complied with. They would not, therefore, be in a position to make submissions to the police after the ICT investigation as to whether or not a criminal investigation was warranted. The applicants asked if, and if so how, the police could establish for themselves whether or not a warrant had been issued, so as to decide whether an investigation was required, and how the police would investigate, assuming there had been no warrant.

9. The DPP responded on 19 October 1999 that the police had to await the ICT decision, and the police responded on 9 November 1999 that the applicants' concerns were receiving the fullest attention, but that they were unable to enter into discussion on matters of internal procedure and inter-departmental investigation.

10. On 21 December 1999 the applicants wrote to the police pointing out that, having received the decision of the ICT, they still did not know whether or not there had been a warrant or whether there had been unlawful interception. The response, dated 17 January 2000, assured the applicants that police officers were making enquires with the relevant agencies with a view to establishing whether there had been a breach of section 1 of the 1985 Act and identifying the appropriate investigative authority. The police informed the applicants by a letter dated 31 March 2000 that their enquiries continued, and, by a letter dated 13 April 2000, that these enquiries had not revealed an offence contrary to section 1 of the 1985 Act.

4. Complaint to the Investigatory Powers Tribunal ("IPT")

11. On 15 December 2000 the former statutory regime for the interception of communications was replaced by the Regulation of Investigatory Powers Act 2000 (see paragraphs 34-39 below) and a new tribunal, the IPT, was created.

12. On 13 August 2001 the applicants began proceedings in the IPT against the security and intelligence agencies of the United Kingdom, complaining of interferences with their rights to privacy for their telephone and other communications from 2 October 2000 onwards (*British-Irish Rights Watch and others v. The Security Service and others*, IPT/01/62/CH). The IPT, sitting as its President and Vice-President (a Court of Appeal and a High Court judge), had security clearance and was able to proceed in the light not just of open evidence filed by the defendant services but also confidential evidence, which could not be made public for reasons of national security.

13. On 9 December 2004 the IPT made a number of preliminary rulings on points of law. Although the applicants had initially formulated a number of claims, by the time of the ruling these had been narrowed down to a single complaint about the lawfulness of the "filtering process", whereby communications between the United Kingdom and an external source, captured under a warrant pursuant to section 8(4) of the 2000 Act (which had replaced section 3(2) of the 1985 Act: see paragraphs 34-39 below), were sorted and accessed pursuant to secret selection criteria. The question was, therefore, whether "the process of filtering intercepted telephone calls made from the UK to overseas telephones ... breaches Article 8 § 2 [of the Convention] because it is not 'in accordance with the law'".

14. The IPT found that the difference between the warrant schemes for interception of internal and external communications was justifiable, because it was more necessary for additional care to be taken with regard to interference with privacy by a Government in relation to domestic telecommunications, given the substantial potential control it exercised in this field; and also because its knowledge of, and control over, external communications was likely to be much less extensive.

15. As to whether the law was sufficiently accessible and foreseeable for the purposes of Article 8 § 2, the IPT observed:

> "The selection criteria in relation to accessing a large quantity of as yet unexamined material obtained pursuant to a s8(4) warrant (as indeed in relation to material obtained in relation to a s8(1) warrant) are those set out in s5(3) . The Complainants' Counsel complains that there is no 'publicly stated material indicating that a relevant person is satisfied that the [accessing] of a particular individual's telephone call is proportionate'. But the Respondents submit that there is indeed such publicly stated material, namely the provisions of s6(l) of the Human Rights Act which requires a public authority to act compatibly with Convention rights, and thus, it is submitted, imposes a duty to act proportionately in applying to the material the s5(3) criteria.
>
> To that duty there is added the existence of seven safeguards listed by the Respondents' Counsel, namely (1) the criminal prohibition on unlawful interception (2) the involvement of the Secretary of State (3) the guiding role of the Joint Intelligence Committee ('JIC') (4) the Code of Practice (5) the oversight by the Interception of Communication Commissioner (whose powers are set out in Part IV of the Act) (6) the availability of proceedings before this Tribunal and (7) the oversight

by the Intelligence and Security Committee, an all-party body of nine Parliamentarians created by the Intelligence Services Act 1994 ...

It is plain that, although in fact the existence of all these safeguards is publicly known, it is not part of the requirements for accessibility or foreseeability that the precise details of those safeguards should be published. The Complainants' Counsel has pointed out that it appears from the Respondents' evidence that there are in existence additional operating procedures, as would be expected given the requirements that there be the extra safeguards required by s16 of the Act, and the obligation of the Secretary of State to ensure their existence under s15(1)(b). It is not suggested by the Complainants that the nature of those operating procedures be disclosed, but that their existence, i.e. something along the lines of what is in the Respondents' evidence, should itself be disclosed in the Code of Practice.

We are unpersuaded by this. First, such a statement in the Code of Practice, namely as to the existence of such procedures, would in fact take the matter no further than it already stands by virtue of the words of the statute. But in any event, the existence of such procedures is only one of the substantial number of safeguards which are known to exist. Accessibility and foreseeability are satisfied by the knowledge of the criteria and the knowledge of the existence of those multiple safeguards.

... [F]oreseeability is only expected to a degree that is reasonable in the circumstances, and the circumstances here are those of national security ... In this case the legislation is adequate and the guidelines are clear. Foreseeability does not require that a person who telephones abroad knows that his conversation is going to be intercepted because of the existence of a valid s. 8(4) warrant. ...

The provisions, in this case the right to intercept and access material covered by a s.8(4) warrant, and the criteria by reference to which it is exercised, are in our judgment sufficiently accessible and foreseeable to be in accordance with law. The parameters in which the discretion to conduct interception is carried on, by reference to s. 5(3) and subject to the safeguards referred to, are plain from the face of the statute. In this difficult and perilous area of national security, taking into account both the necessary narrow approach to Article 8(2) and the fact that the burden is placed upon the Respondent, we are satisfied that the balance is properly struck."

B. Relevant domestic law and practice

1. The Interception of Communications Act 1985

16. During the period at issue in this application the relevant legislation was sections 1-10 of the Interception of Communications Act 1985 ("the 1985 Act"), which came into force on 10 April 1986 and was repealed by the Regulation of Investigatory Powers Act 2000 ("the 2000 Act").

17. Pursuant to section 1 of the 1985 Act, a person who intentionally intercepted a communication in the course of its transmission by post or by means of a public telecommunications system was guilty of an offence. A number of exceptions were made, the relevant one being a communication intercepted pursuant to a warrant issued by the Secretary of State under

section 2 of the 1985 Act and in accordance with a certificate issued under section 3(2)(b) of the 1985 Act.

(a) Warrants for interception

(i) The three grounds for issuing a warrant

18. The Secretary of State's power to issue a warrant under section 2 of the 1985 Act could be exercised only if he considered the warrant necessary:

> "(a) in the interests of national security;
>
> (b) for the purpose of preventing or detecting serious crime; or
>
> (c) for the purpose of safeguarding the economic well-being of the United Kingdom."

19. The term "serious crime" was defined by section 10(3) of the Act as follows:

> "For the purposes of [the 1985 Act], conduct which constitutes or, if it took place in the United Kingdom, would constitute one or more offences shall be regarded as a serious crime if, and only if –
>
> (a) it involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose; or
>
> (b) the offence, or one of the offences, is an offence for which a person who has attained the age of twenty-one and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of three years or more."

20. The scope of the term "national security" was clarified by the Commissioner appointed under the 1985 Act. In his 1986 report he stated (§ 27) that he had adopted the following definition: activities "which threaten the safety or well-being of the State, and which are intended to undermine or overthrow Parliamentary democracy by political, industrial or violent means".

21. In determining whether a warrant was necessary for one of the three reasons set out in section 2(2) of the 1985 Act, the Secretary of State was under a duty to take into account whether the information which it was considered necessary to acquire could reasonably be acquired by other means (section 2(3)). In addition, warrants to safeguard the economic well-being of the United Kingdom could not be issued unless the information to be acquired related to the acts or intentions of persons outside the British Islands (section 2(4)). A warrant required the person to whom it was addressed to intercept, in the course of their transmission by post or by means of a public telecommunications system, such communications as were described in the warrant.

(ii) The two types of warrant

22. Two types of warrant were permitted by section 3 of the 1985 Act. The first, a "section 3(1) warrant", was a warrant that required the interception of:

> "(a) such communications as are sent to or from one or more addresses specified in the warrant, being an address or addresses likely to be used for the transmission of communications to or from–
> (i) one particular person specified or described in the warrant; or
> (ii) one particular set of premises so specified or described; and
>
> (b) such other communications (if any) as it is necessary to intercept in order to intercept communications falling within paragraph (a) above."

By section 10(1) of the 1985 Act, the word "person" was defined to include any organisation or combination of persons and the word "address" was defined to mean any postal or telecommunications address.

23. The second type of warrant, a "section 3(2) warrant", was one that required the interception, in the course of transmission by means of a public telecommunications system, of:

> "(i) such external communications as are described in the warrant; and
>
> (ii) such other communications (if any) as it is necessary to intercept in order to intercept such external communications as are so described ...".

24. When he issued a section 3(2) warrant, the Secretary of State was required to issue also a certificate containing a description of the intercepted material the examination of which he considered necessary in the interests of national security, to prevent or detect serious crime or to safeguard the State's economic well-being (section 3(2)(b)). A section 3(2) warrant could not specify an address in the British Islands for the purpose of including communications sent to or from that address in the certified material unless-

> "3(3) (a) the Secretary of State considers that the examination of communications sent to or from that address is necessary for the purpose of preventing or detecting acts of terrorism; and
>
> (b) communications sent to or from that address are included in the certified material only in so far as they are sent within such a period, not exceeding three months, as is specified in the certificate."

25. Section 3(2) warrants could be issued only under the hand of the Secretary of State or a permitted official of high rank with the written authorisation of the Secretary of State. If issued under the hand of the Secretary of State, the warrant was valid for two months; if by another official, it was valid for two days. Only the Secretary of State could renew a warrant. If the Secretary of State considered that a warrant was no longer necessary in the interests of national security, to prevent or detect serious

crime or to safeguard the State's economic well-being, he was under a duty to cancel it (section 4).

26. The annual report of the Commissioner for 1986 explained the difference between warrants issued under section 3(1) and under section 3(2):

> "There are a number of differences ... But the essential differences may be summarised as follows:
>
> (i) Section 3(2) warrants apply only to external telecommunications;
>
> (ii) whereas section 3(1) warrants only apply to communications to or from one particular person ... or one particular set of premises, Section 3(2) warrants are not so confined; but
>
> (iii) at the time of issuing a Section 3(2) warrant the Secretary of State is obliged to issue a certificate describing the material which it is desired to intercept; and which he regards as necessary to examine for any of the purposes set out in Section 2(2).
>
> So the authority to intercept granted by the Secretary of State under Section 3(2) is limited not so much by reference to the target, as it is under section 3(1), but by reference to the material. It follows that in relation to Section 3(2) warrants, I have had to consider first, whether the warrant applies to external communications only, and, secondly, whether the certified material satisfies the Section 2(2) criteria. ...
>
> There is a further important limitation on Section 3(2) warrants. I have said that the authority granted by the Secretary of State is limited by reference to the material specified in the certificate, rather than the targets named in the warrants. This distinction is further underlined by Section 3(3) which provides that material specified shall *not* include the address in the British Islands for the purpose of including communications sent to or from that address, except in the case of counter-terrorism. So if, for example in a case of subversion the Security Service wishes to intercept external communications to or from a resident of the British Islands, he could not do so under a Section 3(2) warrant by asking for communications sent to or from his address to be included in the certified material. But it would be possible for the Security Service to get indirectly, through a legitimate examination of certified material, what it may not get directly. In such cases it has become the practice to apply for a separate warrant under Section 3(1) known as an overlapping warrant, in addition to the warrant under Section 3(2). There is nothing in the [1985 Act] which requires this to be done. But it is obviously a sound practice, and wholly consistent with the legislative intention underlying Section 3(3). Accordingly I would recommend that where it is desired to intercept communications to or from an individual residing in the British Islands, as a separate target, then in all cases other than counter-terrorism there should be a separate warrant under Section 3(1), even though the communications may already be covered by a warrant under Section 3(3). The point is not without practical importance. For the definition of "relevant warrant" and "relevant certificate" in Section 7(9) of the Act makes it clear that, while the Tribunal has power to investigate warrants issued under section 3(1) and certificates under section 3(2) where an address is specified in the certificate, it has no such power to investigate Section 3(2) warrants, where an address is not so certified."

(iii) Use and retention of information

27. Section 6 of the 1985 Act was entitled "Safeguards" and read as follows:

"(1) Where the Secretary of State issues a warrant he shall, unless such arrangements have already been made, make such arrangements as he considers necessary for the purpose of securing-

(a) that the requirements of subsections (2) and (3) below are satisfied in relation to the intercepted material; and

(b) where a certificate is issued in relation to the warrant, that so much of the intercepted material as is not certified by the certificate is not read, looked at or listened to by any person.

(2) The requirements of this subsection are satisfied in relation to any intercepted material if each of the following, namely-

(a) the extent to which the material is disclosed;

(b) the number of persons to whom any of the material is disclosed;

(c) the extent to which the material is copied; and

(d) the number of copies made of any of the material;

is limited to the minimum that is necessary as mentioned in section 2 (2) above.

(3) The requirements of this subsection are satisfied in relation to any intercepted material if each copy made of any of that material is destroyed as soon as its retention is no longer necessary as mentioned in section 2 (2) above."

(b) The Interception of Communications Tribunal ("ICT")

28. Section 7 of the 1985 Act provided for a Tribunal to investigate complaints from any person who believed that communications sent by or to him had been intercepted. Its jurisdiction, so far as material, was limited to investigating whether there was or had been a "relevant warrant" or a "relevant certificate" and, where there was or had been, whether there had been any contravention of sections 2-5 of the 1985 Act in relation to that warrant or certificate. Section 7(9) read, in so far as relevant, as follows:

"For the purposes of this section –

(a) a warrant is a relevant warrant in relation to an applicant if –

(i) the applicant is specified or described in the warrant; or

(ii) an address used for the transmission of communications to or from a set of premises in the British Islands where the applicant resides or works is so specified;

(b) a certificate is a relevant certificate in relation to an applicant if and to the extent that an address used as mentioned in paragraph (a)(ii) above is specified in the certificate for the purpose of including communications sent to or from that address in the certified material."

29. The ICT applied the principles applicable by a court on an application for judicial review. If it found there had been a contravention of the provisions of the Act, it was to give notice of that finding to the applicant, make a report to the Prime Minister and to the Commissioner appointed under the Act and, where it thought fit, make an order quashing the relevant warrant, directing the destruction of the material intercepted and/or directing the Secretary of State to pay compensation. In other cases, the ICT was to give notice to the applicant stating that there had been no contravention of sections 2-5 of the Act.

30. The ICT consisted of five members, each of whom was required to be a qualified lawyer of not less than ten years standing. They held office for a five-year period and could be re-appointed. The decisions of the ICT were not subject to appeal.

(c) The Commissioner

31. Section 8 provided that a Commissioner be appointed by the Prime Minister. He or she was required to be a person who held, or who had held, high judicial office. The Commissioner's functions included the following:

– to keep under review the carrying out by the Secretary of State of the functions conferred on him by sections 2-5 of the 1985 Act;

– to give to the ICT all such assistance as it might require for the purpose of enabling it to carry out its functions;

– to keep under review the adequacy of the arrangements made under section 6 for safeguarding intercepted material and destroying it where its retention was no longer necessary;

– to report to the Prime Minister if there appeared to have been a contravention of sections 2-5 which had not been reported by the ICT or if the arrangements under section 6 were inadequate;

– to make an annual report to the Prime Minister on the exercise of the Commissioner's functions. This report had to be laid before the Houses of Parliament. The Prime Minister had the power to exclude any matter from the report if publication would have been prejudicial to national security, to the prevention or detection of serious crime or to the well-being of the United Kingdom. The report had to state if any matter had been so excluded.

32. In his first report as Commissioner, in 1992, Sir Thomas Bingham MR, as he then was, explained his own role as part of the safeguards inherent in the 1985 Act as follows:

"The third major safeguard is provided by the Commissioner himself. While there is nothing to prevent consultation of the Commissioner before a warrant is issued, it is

not the practice to consult him in advance and such consultation on a routine basis would not be practicable. So the Commissioner's view is largely retrospective, to check that warrants have not been issued in contravention of the Act and that appropriate procedures were followed. To that end, I have visited all the warrant issuing departments and agencies named in this report, in most cases more than once, and discussed at some length the background to the warrant applications. I have also discussed the procedure for seeking warrants with officials at various levels in all the initiating bodies and presenting departments. I have inspected a significant number of warrants, some chosen by me at random, some put before me because it was felt that I should see them. Although I have described ... a number of instances in which mistakes were made or mishaps occurred, I have seen no case in which the statutory restrictions were deliberately evaded or corners knowingly cut. A salutary practice has grown up by which the Commissioner's attention is specifically drawn to any case in which an error or contravention of the Act has occurred: I accordingly believe that there has been no such case during 1992 of which I am unaware."

Similar conclusions about the authorities' compliance with the law were drawn by all the Commissioners in their reports during the 1990s.

33. In each of the annual reports made under the 1985 Act the Commissioner stated that in his view the arrangements made under section 6 of the 1985 were adequate and complied with, without revealing what the arrangements were. In the 1989 Report the Commissioner noted at § 9 that there had been technological advances in the telecommunications field which had "necessitated the making of further arrangements by the Secretary of State for the safeguarding of material under section 6 of the [1985 Act]". The Commissioner stated that he had reviewed the adequacy of the new arrangements. For the year 1990, the Commissioner recorded that, as a result of a new practice of the police disclosing some material to the Security Service, a further change in the section 6 arrangements had been required. The Commissioner said in the 1990 Report that he was "satisfied with the adequacy of the new arrangements" (1990 Report at § 18). In the 1991 Report, the Commissioner stated that there had been some minor changes to the section 6 arrangements and confirmed that he was satisfied with the arrangements as modified (§ 29 of the 1991 Report). In the 1993 Report, the Commissioner said at § 11:

"Some of the written statements of section 6 safeguards which I inspected required to be updated to take account of changes in the public telecommunications market since they had been drafted and approved. Other statements could, as it seemed to me, be improved by more explicit rules governing the circumstances and manner in which, and the extent to which, intercept material could be copied. It also seemed to me that it would be advantageous, where this was not already done, to remind all involved m handling intercept material on a regular basis of the safeguards to which they were subject, securing written acknowledgements that the safeguards had been read and understood. These suggestions appeared to be readily accepted by the bodies concerned. They did not in my view indicate any failure to comply with section 6 of the Act."

In his first year as Commissioner, Lord Nolan reported the following on this issue of section 6 safeguards (1994 Report, § 6):

> "Like my predecessors, I have on each of my visits considered and discussed the arrangements made by the Secretary of State under section 6 for the purpose of limiting the dissemination and retention of intercepted material to what is necessary within the meaning of section 2. Each agency has its own set of such arrangements, and there are understandable variations between them. For example, the practical considerations involved in deciding what is necessary in the interests of national security, or the economic well-being of the United Kingdom (the areas with which the Security Service and the Secret Intelligence Service are almost exclusively concerned) are somewhat different from those involved in the prevention and detection of serious criminal offences (with which the police forces and HM Customs & Excise are almost exclusively concerned). I am satisfied that all of the agendas are operating within the existing approved safeguards under the terms of the arrangements as they stand ..."

2. The Regulation of Investigatory Powers Act 2000

34. The 2000 Act came into force on 15 December 2000. The explanatory memorandum described the main purpose of the Act as being to ensure that the relevant investigatory powers were used in accordance with human rights. As to the first, interceptions of communications, the 2000 Act repealed, *inter alia*, sections 1-10 of the 1985 Act and provides for a new regime for the interception of communications.

35. The 2000 Act is designed to cover the purposes for which the relevant investigatory powers may be used, which authorities can use the powers, who should authorise each use of the power, the use that can be made of the material gained, judicial oversight and a means of redress for the individual.

36. A new Investigatory Powers Tribunal ("IPT") assumed the responsibilities of the former ICT, of the Security Services Tribunal and of the Intelligence Services Tribunal. The Interception of Communications Commissioner continues to review the actions of the Secretary of State as regards warrants and certificates and to review the adequacy of the arrangements made for the execution of those warrants. He is also, as before, to assist the Tribunal. In addition, the Secretary of State is to consult about and to publish codes of practice relating to the exercise and performance of duties in relation to, *inter alia*, interceptions of communications.

37. Section 2(2) of the 2000 Act defines interception as follows:

> "For the purposes of this Act, but subject to the following provisions of this section, a person intercepts a communication in the course of its transmission by means of a telecommunications system if, and only if, he –
>
> (a) so modifies or interferes with the system, or its operation,
>
> (b) so monitors transmissions made by means of the system, or

(c) so monitors transmissions made by wireless telegraphy to or from apparatus comprised in the system,

as to make some of all of the contents of the communication available, while being transmitted, to a person other than the sender or intended recipient of the communication."

38. Section 5(2) of the 2000 Act provides that the Secretary of State shall not issue an interception warrant unless he believes that the warrant is necessary, *inter alia*, in the interests of national security, for the purpose of preventing or detecting serious crime or for the purpose of safeguarding the economic well-being of the United Kingdom and that the conduct authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

39. In addition to the general safeguards specified in section 15 of the Act, section 16 provides additional safeguards in the case of certificated warrants (namely warrants for interception of external communications supported by a certificate). In particular, section 16(1) provides that intercepted material is to be read, looked at or listened to by the persons to whom it becomes available by virtue of the warrant to the extent only that it has been certified as material the examination of which is necessary for one of the above purposes and falls within subsection (2). Intercepted material falls within subsection (2) so far only as it is selected to be read, looked at or listened to otherwise than according to a factor which is referable to an individual who is known to be for the time being in the British Isles and has as its purpose, or one of its purposes, the identification of material in communications sent by that person, or intended for him.

40. In its Ruling of 9 December 2004 (see paragraphs 13-15 above), the IPT set out the following extracts from the Interception of Communications Code of Practice issued pursuant to s. 71 of the 2000 Act ("the Code of Practice"). Subparagraph 4(2) of the Code of Practice deals with the application for a s. 8(1) warrant as follows :

"An application for a warrant is made to the Secretary of State . . . Each application, a copy of which must be retained by the applicant, should contain the following information :

• Background to the operation in question.

• Person or premises to which the application relates (and how the person or premises feature in the operation) .

• Description of the communications to be intercepted, details of communications service provider(s) and an assessment of the feasibility of the interception operation where this is relevant.

• Description of the conduct to be authorised as considered necessary in order to carry out the interception, where appropriate.

• An explanation of why the interception is considered to be necessary under the provisions of section 5(3).

• A consideration of why the conduct is to be authorised by the warrant is proportionate to what is sought to be achieved by that conduct.

• A consideration of any unusual degree of collateral intrusion and why that intrusion is justified in the circumstances. In particular, where the communications in question might affect religious, medical or journalistic confidentiality or legal privilege, this must be specified in the application.

• Where an application is urgent, supporting justification should be provided.

• An assurance that all material intercepted will be handled in accordance with the safeguards required by section 15 of the Act .

The IPT continued:

"Applications for a s. 8(4) warrant are addressed in subparagraph 5 .2 of the Code of Practice :

'An application for a warrant is made to the Secretary of State ... each application, a copy of which must be retained by the applicant, should contain the following information :

• Background to the operation in question [identical to the first bullet point in 4.2].

• Description of the communications ... [this is materially identical to the third bullet point in 4.1] .

• Description of the conduct to be authorised, which must be restricted to the interception of external communications, or to conduct necessary in order to intercept those external communications, where appropriate [compare the wording of the fourth bullet in 4 .2].

• The certificate that will regulate examination of intercepted material.

• An explanation of why the interception is considered to be necessary for one or more of the section 5(3) purposes [identical to the fifth bullet point in 4 .2].

• A consideration of why the conduct should be authorised by the warrant is proportionate . . . [identical to the sixth bullet point in 4 .2].

• A consideration of any unusual degree of collateral intrusion . . . [identical to the seventh bullet point in 4 .2].

• Where an application is urgent . . . [identical to the eighth bullet point in 4 .2].

• An assurance that intercepted material will be read, looked at or listened to only so far as it is certified, and it meets the conditions of sections 16(2) -16(6) of the Act.

• An assurance that all material intercepted will be handled in accordance with the safeguards required by sections 15 and 16 of the Act [these last two bullets of course are the equivalent to the last bullet point in 4 .2].

... By subparagraph 4(8), the s. 8(I) warrant instrument should include 'the name or description of the interception subject or of the set of premises in relation to which the interception is to take place' and by subparagraph 4(9) there is reference to the schedules required by s. 8(2) of [the 2000 Act]. The equivalent provision in relation to the format of the s. 8(4) warrant in subparagraph 5(9) does not of course identify a particular interception subject or premises, but requires inclusion in the warrant of a 'description of the communications to be intercepted'."

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

41. The applicants complained about the interception of their communications, contrary to Article 8 of the Convention:

"1. Everyone has the right to respect for his private and family life, his home and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

A. The parties' submissions

1. The applicants

42. The applicants complained that, between 1990 and 1997, telephone, facsimile, e-mail and data communications between them were intercepted by the Capenhurst facility, including legally privileged and confidential material.

43. Through the statements of Mr Duncan Campbell, a telecommunications expert, they alleged that the process applying to external warrants under section 3(2) of the 1985 Act embodied five stages.

First, a warrant would be issued, specifying an external communications link or links to be physically intercepted. Such warrants covered very broad classes of communications, for example, "all commercial submarine cables having one terminal in the UK and carrying external commercial

communications to Europe". All communications falling within the specified category would be physically intercepted.

Secondly, the Secretary of State would issue a certificate, describing the categories of information which could be extracted from the total volume of communications intercepted under a particular warrant. Certificates were formulated in general terms, and related only to intelligence tasks and priorities; they did not identify specific targets or addresses. They did not need to be more specific than the broad classes of information specified in the 1985 Act, for example, "national security", "preventing or detecting serious crime" or "safeguarding the economic well-being of the United Kingdom". The combination of a certificate and a warrant formed a "certified warrant".

The third stage in the process was filtering. An automated sorting system or search engine, operating under human control, selected communications containing specific search terms or combinations thereof. The search terms would relate to one or more of the certificates issued for the relevant intercepted communications link. Search terms could also be described as "keyword lists", "technical databases" or "The Dictionary". Search terms and filtering criteria were not specified in certificates, but were selected and administered by State officials without reference to judicial officials or ministers.

Fourth, a system of rules was in place to promote the "minimisation" of the interference with privacy, namely how to review communications intelligence reports and remove names or material identifying citizens or entities whose details might incidentally have been included in raw material which had otherwise been lawfully intercepted and processed. Where the inclusion of such details in the final report was not proportionate or necessary for the lawful purpose of the warranted interception, it would be removed.

The fifth and final stage in the process was "dissemination". Information obtained by an interference with the privacy of communications could be disseminated only where the recipients' purpose(s) in receiving the information was proportionate and necessary in the circumstances. Controls on the dissemination formed a necessary part of Article 8 safeguards.

44. The applicants contended that since the section 3(2) procedure permitted the interception of all communications falling within the large category set out in each warrant, the only protection afforded to those whose communications were intercepted was that the Secretary of State, under section 6(1) of the Act, had to "make such arrangements as he considers necessary for the purpose of securing that ... so much of the intercepted material as is not certified by the certificate is not read, looked at or listened to by any person" unless the requirements of section 6(2) were met. However, the precise nature of these "arrangements" were not, at the relevant time, made known to the public, nor was there any procedure

available to permit an individual to satisfy him or herself that the "arrangements" had been followed. The Tribunal did not have jurisdiction to examine such compliance, and although the Commissioner was authorised under section 8 to review the adequacy of the "arrangements" in general, he had no power to review whether they had been met in an individual case.

45. It was plain that the alleged interception of communications constituted an interference with the applicants' rights under Article 8 § 1. Any such interception, to comply with Article 8 § 2, had to be "in accordance with the law", and thus have a basis in domestic law that was adequately accessible and formulated with sufficient precision as to be foreseeable. They contended that the United Kingdom legislation breached the requirements of foreseeability. They submitted that it would not compromise national security to describe the arrangements in place for filtering and disseminating intercepted material, and that detailed information about similar systems had been published by a number of other democratic countries, such as the United States of America, Australia, New Zealand, Canada and Germany. The deficiencies in the English system were highlighted by the Court's decision in *Weber and Saravia v. Germany* (dec.), no. 54934/00, 29 June 2006, which noted that the German legislation set out on its face detailed provisions regulating, *inter alia*, the way in which individual communications were to be selected from the pool of material derived from "strategic interception"; disclosure of selected material amongst the various agencies of the German State and the use that each could properly make of the material; and the retention or destruction of the material. The authorities' discretion was further regulated and constrained by the public rulings of the Federal Constitutional Court on the compatibility of the provisions with the Constitution. In contrast, in the United Kingdom at the relevant time no provision was made on the face of the statute for any part of the processes following the initial interception, other than the duty on the Secretary of State to make unspecified "arrangements". The arrangements themselves were unpublished. There was no legal material in the public domain indicating how the authorities' powers to select, disclose, use or retain particular communications were regulated. The authorities' conduct was not "in accordance with the law" because it was unsupported by any predictable legal basis satisfying the accessibility principle.

46. In addition, the applicants denied that the interferences pursued a legitimate aim or were proportionate to any such aim, since the 1985 Act permitted interception of large classes of communications for any purpose, and it was only subsequently that this material was sifted to determine whether it fell within the scope of a section 3(2) warrant.

2. The Government

47. For security reasons, the Government adopted a general policy of neither confirming nor denying allegations made in respect of surveillance activities. For the purposes of this application, however, they were content for the Court to proceed on the hypothetical basis that the applicants could rightly claim that communications sent to or from their offices were intercepted at the Capenhurst ETF during the relevant period. Indeed, they submitted that, in principle, any person who sent or received any form of telecommunication outside the British Islands during the period in question could have had such a communication physically intercepted under a section 3(2) warrant. However, the Government emphatically denied that any interception was being conducted without the necessary warrants and it was their position that, if interception of the applicants' communications did occur, it would have been lawfully sanctioned by an appropriate warrant under section 3(2) of the 1985 Act.

48. The Government annexed to their first set of Observations, dated 28 November 2002, a statement by Mr Stephen Boys Smith, a senior Home Office official, in which it was claimed:

> "... Disclosure of the arrangements would reveal important information about the methods of interception used. It is for this reason that the Government is unable to disclose the full detail of the section 6 arrangements for section 3(2) warrants that were in place during the relevant period. The methods to which the relevant documents relate for the relevant period remain a central part of the methods which continue to be used. Therefore, disclosure of the arrangements, the Government assesses and I believe, would be contrary to the interests of national security. It would enable individuals to adapt their conduct so as to minimise the effectiveness of any interception methods which it might be thought necessary to apply to them.
>
> Further, the manuals and instructions setting out the section 6 safeguards and arrangements are in large part not in a form which would be illuminating or readily comprehensible to anyone who had not also undergone the training I have referred to above or had the benefit of detailed explanations. They are couched in technical language and refer to specific techniques and processes which cannot be understood simply from the face of the documents. They contain detailed instructions, precisely in order to ensure that the section 6 arrangements and section 3(2) requirements were fully understood by staff and were fully effective. Any explanations given by the Government of those techniques and processes would compound the problem, referred to above, of undermining the operational effectiveness of the system and techniques used under the authority of warrants."

The Government stressed, however, that the detailed arrangements were the subject of independent review by the successive Commissioners, who reported that they operated as robust safeguards for individuals' rights (see paragraphs 31-33 above).

49. The Government annexed to their Further Observations, dated 23 May 2003, a second statement by Mr Boys Smith, in response to Mr Campbell's statement (see paragraph 48 above), which provided more

detail, to the extent that was possible without undermining national security, about the "arrangements" made by the Secretary of State under section 6 of the Act. The Government submitted that the Court should proceed on the basis that, in the absence of evidence to the contrary, in the democratic society of the United Kingdom, the relevant ministers, officials and Commissioners properly discharged their statutory duties to ensure that safeguards were in place to comply with all the requirements of section 6. Moreover Mr Boys Smith's statement showed that during the relevant period there was a range of safeguards in place to ensure that the process of selection of material for examination (the stage referred to by the applicants as "filtering") could be carried out only strictly in accordance with the statutory framework and the terms of the warrant and the certificate (that is, could be carried out only when necessary in the interests of national security, for the purpose of preventing or detecting serious crime or for the purpose of safeguarding the economic well-being of the United Kingdom), and could not be abused or operated arbitrarily.

50. According to Mr Boys Smith, all persons involved in the selection process would have had their attention specifically drawn to the safeguards and limits set out in the primary legislation, which were rigorously applied. Secondly, training was provided to all these persons to emphasise the importance of strict adherence to the operating procedures and safeguards in place. Thirdly, throughout the relevant period operating procedures were in place to ensure that it was not possible for any single individual to select and examine material on an arbitrary and uncontrolled basis. Where, as part of his intelligence gathering, an official wished to intercept and select relevant information, he could not effect the interception himself. He would have to take the request for interception and selection to personnel in a different branch of the department, who would then separately activate the technical processes necessary for the interception and selection to be made. The requesting official would have to set out, in his request, his justification for the selection. Moreover, a record of the request was kept, so that it was possible for others (senior management and the Commissioner) to check back on the official's request, to ensure that it was properly justified. Conversely, it was not possible for the personnel in the branch of the department implementing the technical interception processes to receive the downloaded product of any interception and selection process implemented by them. Therefore, they also could not conduct unauthorised interception and gain access to material themselves. Fourth, there was day-to-day practical supervision of those who conducted the selection processes under section 3(2) warrants ("the requesting officials") by managers working physically in the same room, who could and would where necessary ask the requesting officials at any time to explain and justify what they were doing. The managers also performed quality control functions in relation to the intelligence reports generated by the requesting officials, and routinely

reviewed all intelligence reports incorporating intercepted material that were drawn up by requesting officials for dissemination. Fifth, throughout the relevant period, as was explained to all personnel involved in the selection process, the independent Commissioner had an unrestricted right to review the operation of the selection process and to examine material obtained pursuant to it. From the relevant records, it was possible to check on the interception initiated by officials and, if necessary, to call for an explanation. Each of the Commissioners during the relevant period (Lords Lloyd, Bingham and Nolan) exercised his right to review the operation of the selection processes, and each Commissioner declared himself satisfied that the selection processes were being conducted in a manner that was fully consistent with the provisions of the 1985 Act. By this combination of measures there were effective safeguards in place against any risk of individual, combined or institutional misbehaviour or action contrary to the terms of the legislation or warrant. Finally, once the Intelligence Services Act 1994 had come into force on 15 December 1994, it was possible for an aggrieved individual to complain to the Tribunal.

51. As regards the processes described by the applicants as "minimisation" and "dissemination", safeguards in place during the relevant period ensured that access to and retention of the raw intercept material and any intelligence reports based on such material were kept to the absolute minimum practicable, having regard to the public interest served by the interception system. Relevant information in the material selected and examined was disseminated in the form of intelligence reports, usually compiled by the requesting officials. As part of the safeguards under section 6 of the 1985 Act, there were throughout the relevant period internal regulations governing the manner in which intelligence reports were produced, directed at all individuals engaged in producing intelligence reports based on material selected from communications intercepted under the section 3(2) warrant regime. The regulations stipulated, among other things, that no information should be reported unless it clearly contributed to a stated intelligence requirement conforming to one of the purposes set out in section 2(2) of the 1985 Act. The regulations also dealt specifically with the circumstances in which it was appropriate to name specific individuals or organisations in the intelligence reports. During the relevant period there was in place a comprehensive security regime for handling all types of classified material. Dissemination was restricted to those with a genuine "need to know", and was further limited to persons who had been security vetted and briefed on how to handle it, with a view to ensuring continued confidentiality.

52. The Government refuted the suggestion that, to comply with Article 8 § 2, the safeguards put in place in respect of the intercepted material had themselves to comply with the "in accordance with the law" criteria. In any event, the functions of the Commissioner and the Tribunal

were embodied in statutory provisions that were sufficiently certain and accessible, and in assessing whether the "foreseeability" requirements of Article 8 § 2 had been met, it was legitimate to take into account the existence of general safeguards against abuse such as these (the Government relied on *Association for European Integration and Human Rights and Ekimzhiev v. Bulgaria,* no. 62540/00, §§ 77-94, 28 June 2007 and *Christie v. the United Kingdom*, no. 21482/93, Commission decision of 27 June 1994). Moreover, the 1985 Act provided that interception was criminal except where the Secretary of State had issued a warrant and sections 2 and 3(2) set out in very clear terms that, during the relevant period, any person in the United Kingdom who sent or received any form of telecommunication outside Britain could in principle have had it intercepted pursuant to such a warrant. The provisions of primary legislation were, therefore, sufficient to provide reasonable notice to individuals to the degree required in this particular context, and provided adequate protection against arbitrary interference. Article 8 § 2 did not require that the nature of the "arrangements" made by the Secretary of State under section 6 of the 1985 Act be set out in legislation (see *Malone v. the United Kingdom*, judgment of 2 August 1984, Series A no. 82, § 68), and for security reasons it had not been possible to reveal such information to the public, but the arrangements had been subject to review by the Commissioners, each of whom had found them to be satisfactory (see paragraph 33 above).

53. The Government submitted that the section 3(2) warrant regime was proportionate and "necessary in a democratic society". Democratic States faced a growing threat from terrorism, and as communications networks became more wide-ranging and sophisticated, terrorist organisations had acquired ever greater scope to operate and co-operate on a trans-national level. It would be a gross dereliction of the Government's duty to safeguard national security and the lives and well-being of its population if it failed to take steps to gather intelligence that might allow preventative action to be taken or if it compromised the operational effectiveness of the surveillance methods available to it. Within the United Kingdom the Government had extensive powers and resources to investigate individuals and organisations that might threaten the interests of national security or perpetrate serious crimes, and it was therefore feasible for the domestic interception regime to require individual addresses to be identified before interception could take place. Outside the jurisdiction, however, the ability of the Government to discover the identity and location of individuals and organisations which might represent a threat to national security was drastically reduced and a broader approach was needed. Maintaining operational effectiveness required not simply that the fact of interception be kept as secret as appropriate; it was also necessary to maintain a degree of secrecy as regards the methods by which such interception might be effected, to prevent the loss of important sources of information.

54. The United Kingdom was not the only signatory to the Convention to make use of a surveillance regime involving the interception of volumes of communications data and the subsequent operation of a process of selection to obtain material for further consideration by government agencies. It was difficult to compare the law and practice of other democratic States (such as the German system of strategic monitoring examined by the Court in the *Weber and Saravia* case cited above), since each country had in place a different set of safeguards. For example, the United Kingdom did not permit intercepted material to be used in court proceedings, whereas many other States did allow this, and there were few, if any, direct equivalents to the independent Commissioner system created by the 1985 Act. Moreover, it was possible that the operational reach of the United Kingdom's system had had to be more extensive, given the high level of terrorist threat directed at the United Kingdom during the period in question.

A. Admissibility

55. The Court notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 of the Convention. It further notes that it is not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

1. Whether there was an interference

56. Telephone, facsimile and e-mail communications are covered by the notions of "private life" and "correspondence" within the meaning of Article 8 (see *Weber and Saravia v. Germany* (dec.), no. 54934/00, § 77, 29 June 2006, and the cases cited therein). The Court recalls its findings in previous cases to the effect that the mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them (see *Weber and Saravia*, cited above, § 78).

57. The Court notes that the Government are prepared to proceed, for the purposes of the present application, on the basis that the applicants can claim to be victims of an interference with their communications sent to or from their offices in the United Kingdom and Ireland. In any event, under

section 3(2) the 1985 Act, the authorities were authorised to capture communications contained within the scope of a warrant issued by the Secretary of State and to listen to and examine communications falling within the terms of a certificate, also issued by the Secretary of State (see paragraphs 23-24 above). Under section 6 of the 1985 Act arrangements had to be made regulating the disclosure, copying and storage of intercepted material (see paragraph 27 above). The Court considers that the existence of these powers, particularly those permitting the examination, use and storage of intercepted communications constituted an interference with the Article 8 rights of the applicants, since they were persons to whom these powers might have been applied (see *Weber and Saravia*, cited above, §§ 78-79).

2. Whether the interference was justified

58. Such an interference is justified by the terms of paragraph 2 of Article 8 only if it is "in accordance with the law", pursues one or more of the legitimate aims referred to in paragraph 2 and is "necessary in a democratic society" in order to achieve the aim or aims (see *Weber and Saravia*, cited above, § 80).

3. *Whether the interference was "in accordance with the law"*

a. General principles

59. The expression "in accordance with the law" under Article 8 § 2 requires, first, that the impugned measure should have some basis in domestic law; it also refers to the quality of the law in question, requiring that it should be compatible with the rule of law and accessible to the person concerned, who must, moreover, be able to foresee its consequences for him (see, among other authorities, *Kruslin v. France*, judgment of 24 April 1990, Series A no. 176-A, § 27; *Huvig v. France*, judgment of 24 April 1990, Series A no. 176-B, § 26; *Lambert v. France*, judgment of 24 August 1998, *Reports of Judgments and Decisions* 1998-V, § 23; *Perry v. the United Kingdom*, no. 63737/00, § 45, ECHR 2003-IX; *Dumitru Popescu v. Romania (No. 2)*, no. 71525/01, § 61, 26 April 2007).

60. It is not in dispute that the interference in question had a legal basis in sections 1-10 of the 1985 Act (see paragraphs 16-27 above). The applicants, however, contended that this law was not sufficiently detailed and precise to meet the "foreseeability" requirement of Article 8(2), given in particular that the nature of the "arrangements" made under section 6(1)(b) was not accessible to the public. The Government responded, relying on paragraph 68 of *Malone* (cited above), that although the scope of the executive's discretion to carry out surveillance had to be indicated in legislation, "the detailed procedures and conditions to be observed do not necessarily have to be incorporated in rules of substantive law".

61. The Court observes, first, that the above passage from *Malone* was itself a reference to *Silver and Others*, also cited above, §§ 88-89. There the Court accepted that administrative Orders and Instructions, which set out the detail of the scheme for screening prisoners' letters but did not have the force of law, could be taken into account in assessing whether the criterion of foreseeability was satisfied in the application of the relevant primary and secondary legislation, but only to "the admittedly limited extent to which those concerned were made sufficiently aware of their contents". It was only on this basis – that the content of the Orders and Instructions were made known to the prisoners – that the Court was able to reject the applicants' contention that the conditions and procedures governing interferences with correspondence, and in particular the directives set out in the Orders and Instructions, should be contained in the substantive law itself.

62. More recently, in its admissibility decision in *Weber and Saravia*, cited above, §§ 93-95, the Court summarised its case-law on the requirement of legal "foreseeability" in this field as follows (and see also *Association for European Integration and Human Rights and Ekimzhiev*, cited above, §§ 75-77):

> "93. .... foreseeability in the special context of secret measures of surveillance, such as the interception of communications, cannot mean that an individual should be able to foresee when the authorities are likely to intercept his communications so that he can adapt his conduct accordingly (see, *inter alia*, *Leander* [*v. Sweden*, judgment of 26 August 1987, Series A no. 116], p. 23, § 51). However, especially where a power vested in the executive is exercised in secret, the risks of arbitrariness are evident (see, *inter alia*, *Malone*, cited above, p. 32, § 67; *Huvig*, cited above, pp. 54-55, § 29; and *Rotaru* [*v. Romania* [GC], no. 28341/95, § 55, ECHR 2000-V]). It is therefore essential to have clear, detailed rules on interception of telephone conversations, especially as the technology available for use is continually becoming more sophisticated (see *Kopp v. Switzerland*, judgment of 25 March 1998, *Reports* 1998-II, pp. 542-43, § 72, and *Valenzuela Contreras v. Spain*, judgment of 30 July 1998, *Reports* 1998-V, pp. 1924-25, § 46). The domestic law must be sufficiently clear in its terms to give citizens an adequate indication as to the circumstances in which and the conditions on which public authorities are empowered to resort to any such measures (see *Malone*, ibid.; *Kopp*, cited above, p. 541, § 64; *Huvig*, cited above, pp. 54-55, § 29; and *Valenzuela Contreras*, ibid.).
>
> 94. Moreover, since the implementation in practice of measures of secret surveillance of communications is not open to scrutiny by the individuals concerned or the public at large, it would be contrary to the rule of law for the legal discretion granted to the executive or to a judge to be expressed in terms of an unfettered power. Consequently, the law must indicate the scope of any such discretion conferred on the competent authorities and the manner of its exercise with sufficient clarity to give the individual adequate protection against arbitrary interference (see, among other authorities, *Malone*, cited above, pp. 32-33, § 68; *Leander*, cited above, p. 23, § 51; and *Huvig*, cited above, pp. 54-55, § 29).
>
> 95. In its case-law on secret measures of surveillance, the Court has developed the following minimum safeguards that should be set out in statute law in order to avoid abuses of power: the nature of the offences which may give rise to an interception

141

order; a definition of the categories of people liable to have their telephones tapped; a limit on the duration of telephone tapping; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when communicating the data to other parties; and the circumstances in which recordings may or must be erased or the tapes destroyed (see, *inter alia*, *Huvig*, cited above, p. 56, § 34; *Amann*, cited above, § 76; *Valenzuela Contreras*, cited above, pp. 1924-25, § 46; and *Prado Bugallo v. Spain*, no. 58496/00, § 30, 18 February 2003)."

63. It is true that the above requirements were first developed by the Court in connection with measures of surveillance targeted at specific individuals or addresses (the equivalent, within the United Kingdom, of the section 3(1) regime). However, the *Weber and Saravia* case was itself concerned with generalised "strategic monitoring", rather than the monitoring of individuals (cited above, § 18). The Court does not consider that there is any ground to apply different principles concerning the accessibility and clarity of the rules governing the interception of individual communications, on the one hand, and more general programmes of surveillance, on the other. The Court's approach to the foreseeability requirement in this field has, therefore, evolved since the Commission considered the United Kingdom's surveillance scheme in its above-cited decision in *Christie v. the United Kingdom*.

b. Application of the general principles to the present case

64. The Court recalls that section 3(2) of the 1985 Act allowed the executive an extremely broad discretion in respect of the interception of communications passing between the United Kingdom and an external receiver, namely to intercept "such external communications as are described in the warrant". There was no limit to the type of external communications which could be included in a section 3(2) warrant. According to the applicants, warrants covered very broad classes of communications, for example, "all commercial submarine cables having one terminal in the UK and carrying external commercial communications to Europe", and all communications falling within the specified category would be physically intercepted (see paragraph 43 above). In their observations to the Court, the Government accepted that, in principle, any person who sent or received any form of telecommunication outside the British Islands during the period in question could have had such a communication intercepted under a section 3(2) warrant (see paragraph 47 above). The legal discretion granted to the executive for the physical capture of external communications was, therefore, virtually unfettered.

65. Moreover, the 1985 Act also conferred a wide discretion on the State authorities as regards which communications, out of the total volume of those physically captured, were listened to or read. At the time of issuing a section 3(2) interception warrant, the Secretary of State was required to issue a certificate containing a description of the intercepted material which he considered should be examined. Again, according to the applicants,

certificates were formulated in general terms and related only to intelligence tasks and priorities, such as, for example, "national security", "preventing or detecting serious crime" or "safeguarding the economic well-being of the United Kingdom" (see paragraph 43 above). On the face of the 1985 Act, only external communications emanating from a particular address in the United Kingdom could not be included in a certificate for examination unless the Secretary of State considered it necessary for the prevention or detection of acts of terrorism (see paragraphs 23-24 above). Otherwise, the legislation provided that material could be contained in a certificate, and thus listened to or read, if the Secretary of State considered this was required in the interests of national security, the prevention of serious crime or the protection of the United Kingdom's economy.

66. Under section 6 of the 1985 Act, the Secretary of State, when issuing a warrant for the interception of external communications, was called upon to "make such arrangements as he consider[ed] necessary" to ensure that material not covered by the certificate was not examined and that material that was certified as requiring examination was disclosed and reproduced only to the extent necessary. The applicants contend that material was selected for examination by an electronic search engine, and that search terms, falling within the broad categories covered by the certificates, were selected and operated by officials (see paragraph 43 above). According to the Government (see paragraphs 48-51 above), there were at the relevant time internal regulations, manuals and instructions applying to the processes of selection for examination, dissemination and storage of intercepted material, which provided a safeguard against abuse of power. The Court observes, however, that details of these "arrangements" made under section 6 were not contained in legislation or otherwise made available to the public.

67. The fact that the Commissioner in his annual reports concluded that the Secretary of State's "arrangements" had been complied with (see paragraphs 32-33 above), while an important safeguard against abuse of power, did not contribute towards the accessibility and clarity of the scheme, since he was not able to reveal what the "arrangements" were. In this connection the Court recalls its above case-law to the effect that the procedures to be followed for examining, using and storing intercepted material, *inter alia*, should be set out in a form which is open to public scrutiny and knowledge.

68. The Court notes the Government's concern that the publication of information regarding the arrangements made by the Secretary of State for the examination, use, storage, communication and destruction of intercepted material during the period in question might have damaged the efficacy of the intelligence-gathering system or given rise to a security risk. However, it observes that the German authorities considered it safe to include in the G10 Act, as examined in *Weber and Saravia* (cited above), express provisions

about the treatment of material derived from strategic interception as applied to non-German telephone connections. In particular, the G10 Act stated that the Federal Intelligence Service was authorised to carry out monitoring of communications only with the aid of search terms which served, and were suitable for, the investigation of the dangers described in the monitoring order and which search terms had to be listed in the monitoring order (op. cit., § 32). Moreover, the rules on storing and destroying data obtained through strategic monitoring were set out in detail in section 3(6) and (7) and section 7(4) of the amended G10 Act (see *Weber and Saravia,* cited above, § 100). The authorities storing the data had to verify every six months whether those data were still necessary to achieve the purposes for which they had been obtained by or transmitted to them. If that was not the case, they had to be destroyed and deleted from the files or, at the very least, access to them had to be blocked; the destruction had to be recorded in minutes and, in the cases envisaged in section 3(6) and section 7(4), had to be supervised by a staff member qualified to hold judicial office. The G10 Act further set out detailed provisions governing the transmission, retention and use of data obtained through the interception of external communications (op. cit., §§ 33-50). In the United Kingdom, extensive extracts from the Code of Practice issued under section 71 of the 2000 Act are now in the public domain (see paragraph 40 above), which suggests that it is possible for a State to make public certain details about the operation of a scheme of external surveillance without compromising national security.

69. In conclusion, the Court does not consider that the domestic law at the relevant time indicated with sufficient clarity, so as to provide adequate protection against abuse of power, the scope or manner of exercise of the very wide discretion conferred on the State to intercept and examine external communications. In particular, it did not, as required by the Court's case-law, set out in a form accessible to the public any indication of the procedure to be followed for selecting for examination, sharing, storing and destroying intercepted material. The interference with the applicants' rights under Article 8 was not, therefore, "in accordance with the law".

70. It follows that there has been a violation of Article 8 in this case.

II. ALLEGED VIOLATION OF ARTICLE 13 OF THE CONVENTION

71. The applicants also complained under Article 13, which provides:

> "Everyone whose rights and freedoms as set forth in [the] Convention are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity."

They submitted that Article 13 required the provision of a domestic remedy allowing the competent national authority to deal with the substance

of the Convention complaint and to grant relief. The 1985 Act, however, provided no remedy for an interference where there had been a breach of the section 6 "arrangements" in a particular case.

A. Admissibility

72. The Court notes that this complaint is not manifestly ill-founded within the meaning of Article 35 § 3 of the Convention. It further notes that it is not inadmissible on any other grounds. It must therefore be declared admissible.

B. Merits

73. However, in the light of its above finding that the system for interception of external communications under the 1985 Act was not formulated with sufficient clarity to give the individual adequate protection against arbitrary interference, the Court does not consider that it is necessary to examine separately the complaint under Article 13.

III. APPLICATION OF ARTICLE 41 OF THE CONVENTION

74. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

A. Damage

75. The applicant submitted that the application related to allegations of unlawful interception of communications over a period of approximately seven years (1990-1997), and claimed EUR 3,000 each, making a total of EUR 9,000 in respect of non-pecuniary damage.

76. The Government referred to a number of other cases involving covert surveillance where the Court held that the finding of a violation was sufficient just satisfaction (*Khan v. the United Kingdom*, no. 35394/97, ECHR 2000-V; *Armstrong v. the United Kingdom*, no. 48521/99, 16 July 2002; *Taylor-Sabori v. the United Kingdom*, no. 47114/99, 22 October 2002; *Hewitson v. the United Kingdom*, no. 50015/99, 29 May 2003; *Chalkley v. the United Kingdom*, no. 63831/00, 12 June 2003) and submitted that no financial compensation for non-pecuniary damage would be necessary in the present case.

77. In the circumstances of this case, the Court considers that the finding of violation constitutes sufficient just satisfaction for any non-pecuniary damage caused to the applicants.

B. Costs and expenses

78. The applicant also claimed GBP 7,596, excluding value added tax ("VAT") for the costs and expenses incurred before the Court.

79. The Government noted that counsel had acted throughout on a *pro bono* basis, and submitted that the GBP 180 hourly rate charged by Liberty was excessive. They proposed that GBP 120 per hour would be more reasonable, giving a total of GBP 5,064.

80. The Court awards EUR 7,500 plus any VAT that may be chargeable.

C. Default interest

81. The Court considers it appropriate that the default interest should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT UNANIMOUSLY

1. *Declares* the application admissible;

2. *Holds* that there has been a violation of Article 8 of the Convention;

3. *Holds* that there is no need to examine the complaint under Article 13 of the Convention;

4. *Holds*
   (a) that the respondent State is to pay the applicant, within three months from the date on which the judgment becomes final in accordance with Article 44 § 2 of the Convention, EUR 7,500 (seven thousand five hundred euros) in respect of costs and expenses, to be converted into pounds sterling at the rate applicable at the date of settlement, plus any tax that may be chargeable to the applicants;
   (b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

5. *Dismisses* the remainder of the applicant's claim for just satisfaction.

146

Done in English, and notified in writing on 1 July 2008, pursuant to Rule 77 §§ 2 and 3 of the Rules of Court.

Lawrence Early
Registrar

Lech Garlicki
President

147

CONSEIL DE L'EUROPE

COUNCIL OF EUROPE

COUR EUROPÉENNE DES DROITS DE L'HOMME
EUROPEAN COURT OF HUMAN RIGHTS

GRAND CHAMBER

CASE OF S. AND MARPER v. THE UNITED KINGDOM

(Applications nos. 30562/04 and 30566/04)

JUDGMENT

STRASBOURG

4 December 2008

148

In the case of S. and Marper v. the United Kingdom,

The European Court of Human Rights, sitting as a Grand Chamber composed of:

Jean-Paul Costa, *President,*
Christos Rozakis,
Nicolas Bratza,
Peer Lorenzen,
Françoise Tulkens,
Josep Casadevall,
Giovanni Bonello,
Corneliu Bîrsan,
Nina Vajić,
Anatoly Kovler,
Stanislav Pavlovschi,
Egbert Myjer,
Danutė Jočienė,
Ján Šikuta,
Mark Villiger,
Päivi Hirvelä,
Ledi Bianku, *judges,*

and Michael O'Boyle, *Deputy Registrar*,

Having deliberated in private on 27 February and 12 November 2008,

Delivers the following judgment, which was adopted on the last-mentioned date:

PROCEDURE

1. The case originated in two applications (nos. 30562/04 and 30566/04) against the United Kingdom of Great Britain and Northern Ireland lodged with the Court under Article 34 of the Convention for the Protection of Human Rights and Fundamental Freedoms ("the Convention") by two British nationals, Mr S. ("the first applicant") and Mr Michael Marper ("the second applicant"), on 16 August 2004. The President of the Grand Chamber acceded to the first applicant's request not to have his name disclosed (Rule 47 § 3 of the Rules of Court).

2. The applicants, who were granted legal aid, were represented by Mr P. Mahy of Messrs Howells, a solicitor practising in Sheffield. The United Kingdom Government ("the Government") were represented by their Agent, Mr J. Grainger, Foreign and Commonwealth Office.

3. The applicants complained under Articles 8 and 14 of the Convention that the authorities had continued to retain their fingerprints and cellular

samples and DNA profiles after the criminal proceedings against them had ended with an acquittal or had been discontinued.

4. The applications were allocated to the Fourth Section of the Court (Rule 52 § 1). On 16 January 2007 they were declared admissible by a Chamber of that Section composed of Josep Casadevall, President, Nicolas Bratza, Giovanni Bonello, Kristaq Traja, Stanislav Pavlovschi, Ján Šikuta, Päivi Hirvelä, judges, and Lawrence Early, Section Registrar.

5. On 10 July 2007 the Chamber relinquished jurisdiction in favour of the Grand Chamber, neither party having objected to relinquishment (Article 30 of the Convention and Rule 72).

6. The composition of the Grand Chamber was determined according to the provisions of Article 27 §§ 2 and 3 of the Convention and Rule 24.

7. The applicants and the Government each filed memorials on the merits. In addition, third-party submissions were received from Ms A. Fairclough on behalf of the National Council for Civil Liberties ("Liberty") and from Covington and Burling LLP on behalf of Privacy International, who had been granted leave by the President to intervene in the written procedure (Article 36 § 2 of the Convention and Rule 44 § 2). Both parties replied to Liberty's submissions, and the Government also replied to the comments by Privacy International (Rule 44 § 5).

8. A hearing took place in public in the Human Rights Building, Strasbourg, on 27 February 2008 (Rule 59 § 3).

There appeared before the Court:

(a) *for the Government*

Mrs	E. WILLMOTT,	*Agent*,
Mr	RABINDER SINGH QC,	
Mr	J. STRACHAN,	*Counsel*,
Mr	N. FUSSELL,	
Ms	P. MCFARLANE,	
Mr	M. PRIOR,	
Mr	S. BRAMBLE,	
Ms	E. REES,	
Mr	S. SEN,	*Advisers*,
Mr	D. GOURLEY,	
Mr	D. LOVEDAY,	*Observers*;

(b) *for the applicants*

Mr	S. CRAGG,	
Mr	A. SUTERWALLA,	*Counsel*,
Mr	P. MAHY,	*Solicitor*.

150

The Court heard addresses by Mr Cragg and Mr Rabinder Singh QC, as well as their answers to questions put by the Court.

THE FACTS

I. THE CIRCUMSTANCES OF THE CASE

9. The applicants were born in 1989 and 1963 respectively and live in Sheffield.

10. The first applicant, Mr S., was arrested on 19 January 2001 at the age of 11 and charged with attempted robbery. His fingerprints and DNA samples[1] were taken. He was acquitted on 14 June 2001.

11. The second applicant, Mr Michael Marper, was arrested on 13 March 2001 and charged with harassment of his partner. His fingerprints and DNA samples were taken. Before a pre-trial review took place, he and his partner had reconciled, and the charge was not pressed. On 11 June 2001, the Crown Prosecution Service served a notice of discontinuance on the applicant's solicitors, and on 14 June 2001 the case was formally discontinued.

12. Both applicants asked for their fingerprints and DNA samples to be destroyed, but in both cases the police refused. The applicants applied for judicial review of the police decisions not to destroy the fingerprints and samples. On 22 March 2002 the Administrative Court (Rose LJ and Leveson J) rejected the application [[2002] EWHC 478 (Admin)].

13. On 12 September 2002 the Court of Appeal upheld the decision of the Administrative Court by a majority of two (Lord Woolf CJ and Waller LJ) to one (Sedley LJ) [[2003] EWCA Civ 1275]. As regards the necessity of retaining DNA samples, Lord Justice Waller stated:

> "... [F]ingerprints and DNA *profiles* reveal only limited personal information. The physical samples potentially contain very much greater and more personal and detailed information. The anxiety is that science may one day enable analysis of samples to go so far as to obtain information in relation to an individual's propensity to commit certain crime and be used for that purpose within the language of the present section [section 82 of the Criminal Justice and Police Act 2001]. It might also be said that the law might be changed in order to allow the samples to be used for purposes other than those identified by the section. It might also be said that while

1. DNA stands for deoxyribonucleic acid; it is the chemical found in virtually every cell in the body and the genetic information therein, which is in the form of a code or language, determines physical characteristics and directs all the chemical processes in the body. Except for identical twins, each person's DNA is unique. DNA samples are cellular samples and any subsamples or part samples retained from these after analysis. DNA profiles are digitised information which is stored electronically on the National DNA Database together with details of the person to whom it relates.

samples are retained there is even now a risk that they will be used in a way that the law does not allow. So, it is said, the aims could be achieved in a less restrictive manner ... Why cannot the aim be achieved by retention of the profiles without retention of the samples?

The answer to [these] points is as I see it as follows. First the retention of samples permits (a) the checking of the integrity and future utility of the DNA database system; (b) a reanalysis for the upgrading of DNA profiles where new technology can improve the discriminating power of the DNA matching process; (c) reanalysis and thus an ability to extract other DNA markers and thus offer benefits in terms of speed, sensitivity and cost of searches of the database; (d) further analysis in investigations of alleged miscarriages of justice; and (e) further analysis so as to be able to identify any analytical or process errors. It is these benefits which must be balanced against the risks identified by Liberty. In relation to those risks, the position in any event is first that any change in the law will have to be itself Convention compliant; second any change in practice would have to be Convention compliant; and third unlawfulness must not be assumed. In my view thus the risks identified are not great, and such as they are they are outweighed by the benefits in achieving the aim of prosecuting and preventing crime."

14. Lord Justice Sedley considered that the power of a chief constable to destroy data which he would ordinarily retain had to be exercised in every case, however rare such cases might be, where he or she was satisfied on conscientious consideration that the individual was free of any taint of suspicion. He also noted that the difference between the retention of samples and DNA profiles was that the retention of samples would enable more information to be derived than had previously been possible.

15. On 22 July 2004 the House of Lords dismissed an appeal by the applicants. Lord Steyn, giving the lead judgment, noted the legislative history of section 64(1A) of the Police and Criminal Evidence Act 1984 (PACE), in particular the way in which it had been introduced by Parliament following public disquiet about the previous law, which had provided that where a person was not prosecuted or was acquitted of offences, the sample had to be destroyed and the information could not be used. In two cases, compelling DNA evidence linking one suspect to a rape and another to a murder had not been able to be used, as at the time the matches were made both defendants had either been acquitted or a decision made not to proceed for the offences for which the profiles had been obtained: as a result it had not been possible to convict either suspect.

16. Lord Steyn noted that the value of retained fingerprints and samples taken from suspects was considerable. He gave the example of a case in 1999, in which DNA information from the perpetrator of a crime was matched with that of "I" in a search of the national database. The sample from "I" should have been destroyed, but had not been. "I" had pleaded guilty to rape and was sentenced. If the sample had not been wrongly detained, the offender might have escaped detection.

17. Lord Steyn also referred to statistical evidence from which it appeared that almost 6,000 DNA profiles had been linked with crime-scene

stain profiles which would have been destroyed under the former provisions. The offences involved included 53 murders, 33 attempted murders, 94 rapes, 38 sexual offences, 63 aggravated burglaries and 56 cases involving the supply of controlled drugs. On the basis of the existing records, the Home Office statistics estimated that there was a 40% chance that a crime-scene sample would be matched immediately with an individual's profile on the national database. This showed that the fingerprints and samples which could now be retained had in the previous three years played a major role in the detection and prosecution of serious crime.

18. Lord Steyn also noted that PACE dealt separately with the taking of fingerprints and samples, their retention and their use.

19. As to the Convention analysis, Lord Steyn inclined to the view that the mere retention of fingerprints and DNA samples did not constitute an interference with the right to respect for private life but stated that, if he were wrong in that view, he regarded any interference as very modest indeed. Questions of whether, in the future, retained samples could be misused were not relevant in respect of contemporary use of retained samples in connection with the detection and prosecution of crime. If future scientific developments required it, judicial decisions could be made, when the need occurred, to ensure compatibility with the Convention. The provision limiting the permissible use of retained material to "*purposes related to* the prevention or detection of crime ..." did not broaden the permitted use unduly, because it was limited by its context.

20. If the need to justify the modest interference with private life arose, Lord Steyn agreed with Lord Justice Sedley in the Court of Appeal that the purposes of retention – the prevention of crime and the protection of the right of others to be free from crime – were "provided for by law", as required by Article 8 of the Convention.

21. As to the justification for any interference, the applicants had argued that the retention of fingerprints and DNA samples created suspicion in respect of persons who had been acquitted. Counsel for the Home Secretary had contended that the aim of the retention had nothing to do with the past, that is, with the offence of which a person had been acquitted, but was to assist in the investigation of offences in the future. The applicants would only be affected by the retention of the DNA samples if their profiles matched those found at the scene of a future crime. Lord Steyn saw five factors which led to the conclusion that the interference was proportionate to the aim: (i) the fingerprints and samples were kept only for the limited purpose of the detection, investigation and prosecution of crime; (ii) the fingerprints and samples were not of any use without a comparator fingerprint or sample from the crime scene; (iii) the fingerprints would not be made public; (iv) a person was not identifiable from the retained material to the untutored eye; (v) the resultant expansion of the national database by

the retention conferred enormous advantages in the fight against serious crime.

22. In reply to the contention that the same legislative aim could be obtained by less intrusive means, namely by a case-by-case consideration of whether or not to retain fingerprints and samples, Lord Steyn referred to Lord Justice Waller's comments in the Court of Appeal, which read as follows:

> "If justification for retention is in any degree to be by reference to the view of the police on the degree of innocence, then persons who have been acquitted and have their samples retained can justifiably say this stigmatises or discriminates against me – I am part of a pool of acquitted persons presumed to be innocent, but I am treated as though I was not. It is not in fact in any way stigmatising someone who has been acquitted to say simply that samples lawfully obtained are retained as the norm, and it is in the public interest in its fight against crime for the police to have as large a database as possible."

23. Lord Steyn did not accept that the difference between samples and DNA profiles affected the position.

24. The House of Lords further rejected the applicants' complaint that the retention of their fingerprints and samples subjected them to discriminatory treatment in breach of Article 14 of the Convention when compared to the general body of persons who had not had their fingerprints and samples taken by the police in the course of a criminal investigation. Lord Steyn held that, even assuming that the retention of fingerprints and samples fell within the ambit of Article 8 of the Convention so as to trigger the application of Article 14, the difference of treatment relied on by the applicants was not one based on "status" for the purposes of Article 14: the difference simply reflected the historical fact, unrelated to any personal characteristic, that the authorities already held the fingerprints and samples of the individuals concerned which had been lawfully taken. The applicants and their suggested comparators could not in any event be said to be in an analogous situation. Even if, contrary to his view, it was necessary to consider the justification for any difference in treatment, Lord Steyn held that such objective justification had been established: firstly, the element of legitimate aim was plainly present, as the increase in the database of fingerprints and samples promoted the public interest by the detection and prosecution of serious crime and by exculpating the innocent; secondly, the requirement of proportionality was satisfied, section 64(1A) of PACE objectively representing a measured and proportionate response to the legislative aim of dealing with serious crime.

25. Baroness Hale of Richmond disagreed with the majority, considering that the retention of both fingerprint and DNA data constituted an interference by the State in a person's right to respect for his private life and thus required justification under the Convention. In her opinion, this was an aspect of what had been called informational privacy and there could be

little, if anything, more private to the individual than the knowledge of his genetic make-up. She further considered that the difference between fingerprint and DNA data became more important when it came to justify their retention as the justifications for each of these might be very different. She agreed with the majority that such justifications had been readily established in the applicants' cases.

II. RELEVANT DOMESTIC LAW AND MATERIALS

A. England and Wales

1. Police and Criminal Evidence Act 1984 (PACE)

26. PACE contains powers for the taking of fingerprints (principally section 61) and samples (principally section 63). By section 61, fingerprints may only be taken without consent if an officer of at least the rank of superintendent authorises the taking, or if the person has been charged with a recordable offence or has been informed that he will be reported for such an offence. Before fingerprints are taken, the person must be informed that the prints may be the subject of a speculative search, and the fact of the informing must be recorded as soon as possible. The reason for the taking of the fingerprints is recorded in the custody record. Parallel provisions relate to the taking of samples (section 63).

27. As to the retention of such fingerprints and samples (and the records thereof), section 64(1A) of PACE was substituted by section 82 of the Criminal Justice and Police Act 2001. It provides as follows:

> "Where (a) fingerprints or samples are taken from a person in connection with the investigation of an offence; and (b) subsection (3) below does not require them to be destroyed, the fingerprints or samples may be retained after they have fulfilled the purposes for which they were taken but shall not be used by any person except for purposes related to the prevention or detection of crime, the investigation of an offence, or the conduct of a prosecution. ...
>
> (3) If (a) fingerprints or samples are taken from a person in connection with the investigation of an offence; and (b) that person is not suspected of having committed the offence, they must, except as provided in the following provisions of this section, be destroyed as soon as they have fulfilled the purpose for which they were taken.
>
> (3AA) Samples and fingerprints are not required to be destroyed under subsection (3) above if (a) they were taken for the purposes of the investigation of an offence of which a person has been convicted; and (b) a sample or, as the case may be, fingerprint was also taken from the convicted person for the purposes of that investigation."

28. Section 64 in its earlier form had included a requirement that if the person from whom the fingerprints or samples were taken in connection with the investigation was acquitted of that offence, the fingerprints and

samples, subject to certain exceptions, were to be destroyed "as soon as practicable after the conclusion of the proceedings".

29. The subsequent use of materials retained under section 64(1A) is not regulated by statute, other than the limitation on use contained in that provision. In *Attorney-General's Reference (No. 3 of 1999)* [2001] 2 AC 91, the House of Lords had to consider whether it was permissible to use in evidence a sample which should have been destroyed under the then text of section 64 of PACE. The House considered that the prohibition on the use of an unlawfully retained sample "for the purposes of any investigation" did not amount to a mandatory exclusion of evidence obtained as a result of a failure to comply with the prohibition, but left the question of admissibility to the discretion of the trial judge.

2. Data Protection Act 1998

30. The Data Protection Act was adopted on 16 July 1998 to give effect to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (see paragraph 50 below). Under the Data Protection Act "personal data" means data which relate to a living individual who can be identified (a) from those data; or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual (section 1). "Sensitive personal data" means personal data consisting, *inter alia*, of information as to the racial or ethnic origin of the data subject, the commission or alleged commission by him of any offence, or any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings (section 2).

31. The Act stipulates that the processing of personal data is subject to eight data protection principles listed in Schedule 1. Under the first principle personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless (a) at least one of the conditions in Schedule 2 is met; and (b) in case of sensitive personal data, at least one of the conditions in Schedule 3 is also met. Schedule 2 contains a detailed list of conditions, and provides, *inter alia*, that the processing of any personal data is necessary for the administration of justice or for the exercise of any other functions of a public nature exercised in the public interest by any person (§ 5 (a) and (d)). Schedule 3 contains a more detailed list of conditions, including that the processing of sensitive personal data is necessary for the purpose of, or in connection with, any legal proceedings (§ 6 (a)), or for the administration of justice (§ 7 (a)), and is carried out with appropriate safeguards for the rights and freedoms of data subjects (§ 4 (b)). Section 29 notably provides that personal data processed for the prevention or detection of crime are exempt from the first principle except to the extent to which it

requires compliance with the conditions in Schedules 2 and 3. The fifth principle stipulates that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

32. The Information Commissioner created pursuant to the Act (as amended) has an independent duty to promote the following of good practice by data controllers and has power to make orders ("enforcement notices") in this respect (section 40). The Act makes it a criminal offence not to comply with an enforcement notice (section 47) or to obtain or disclose personal data or information contained therein without the consent of the data controller (section 55). Section 13 affords a right to claim damages in the domestic courts in respect of contraventions of the Act.

3. Retention Guidelines for Nominal Records on the Police National Computer 2006

33. A set of guidelines for the retention of fingerprint and DNA information is contained in the Retention Guidelines for Nominal Records on the Police National Computer 2006 drawn up by the Association of Chief Police Officers in England and Wales. The Guidelines are based on a format of restricting access to the Police National Computer (PNC) data, rather than the deletion of that data. They recognise that their introduction may thus have implications for the business of the non-police agencies with which the police currently share PNC data.

34. The Guidelines set various degrees of access to the information contained on the PNC through a process of "stepping down" access. Access to information concerning persons who have not been convicted of an offence is automatically "stepped down" so that this information is only open to inspection by the police. Access to information about convicted persons is likewise "stepped down" after the expiry of certain periods of time ranging from five to thirty-five years, depending on the gravity of the offence, the age of the suspect and the sentence imposed. For certain convictions the access will never be "stepped down".

35. Chief police officers are the data controllers of all PNC records created by their force. They have the discretion in exceptional circumstances to authorise the deletion of any conviction, penalty notice for disorder, acquittal or arrest histories "owned" by them. An "exceptional case procedure" to assist chief police officers in relation to the exercise of this discretion is set out in Appendix 2. It is suggested that exceptional cases are rare by definition and include those where the original arrest or sampling was unlawful or where it is established beyond doubt that no offence existed. Before deciding whether a case is exceptional, the chief police officer is instructed to seek advice from the DNA and Fingerprint Retention Project.

B. Scotland

36. Under the 1995 Criminal Procedure Act of Scotland, as subsequently amended, the DNA samples and resulting profiles must be destroyed if the individual is not convicted or is granted an absolute discharge. A recent qualification provides that biological samples and profiles may be retained for three years, if the arrestee is suspected of certain sexual or violent offences even if a person is not convicted (section 83 of the 2006 Act, adding section 18A to the 1995 Act.). Thereafter, samples and information are required to be destroyed unless a chief constable applies to a sheriff for a two-year extension.

C. Northern Ireland

37. The Police and Criminal Evidence Order of Northern Ireland 1989 was amended in 2001 in the same way as PACE applicable in England and Wales. The relevant provisions currently governing the retention of fingerprint and DNA data in Northern Ireland are identical to those in force in England and Wales (see paragraph 27 above).

D. Nuffield Council on Bioethics' report[1]

38. According to a recent report by the Nuffield Council on Bioethics, the retention of fingerprints, DNA profiles and biological samples is generally more controversial than the taking of such bioinformation, and the retention of biological samples raises greater ethical concerns than digitised DNA profiles and fingerprints, given the differences in the level of information that could be revealed. The report referred, in particular, to the lack of satisfactory empirical evidence to justify the present practice of retaining indefinitely fingerprints, samples and DNA profiles from all those arrested for a recordable offence, irrespective of whether they were subsequently charged or convicted. The report voiced particular concerns at the policy of permanently retaining the bioinformation of minors, having regard to the requirements of the 1989 United Nations Convention on the Rights of the Child.

39. The report also expressed concerns at the increasing use of the DNA data for familial searching, inferring ethnicity and non-operational research. Familial searching is the process of comparing a DNA profile from a crime scene with profiles stored on the national database, and prioritising them in

1. The Nuffield Council on Bioethics is an independent expert body composed of clinicians, lawyers, philosophers, scientists and theologians established by the Nuffield Foundation in 1991. The present report was published on 18 September 2007 under the following title, *The Forensic Use of Bioinformation: Ethical Issues*.

terms of "closeness" to a match. This allows possible genetic relatives of an offender to be identified. Familial searching might thus lead to revealing previously unknown or concealed genetic relationships. The report considered the use of the DNA database in searching for relatives as particularly sensitive.

40. The particular combination of alleles[1] in a DNA profile can furthermore be used to assess the most likely ethnic origin of the donor. Ethnic inferring through DNA profiles is possible as the individual "ethnic appearance" is systematically recorded on the database: when taking biological samples, police officers routinely classify suspects into one of seven "ethnic appearance" categories. Ethnicity tests on the database might thus provide inferences for use during a police investigation in order, for example, to help reduce a "suspect pool" and to inform police priorities. The report noted that social factors and policing practices lead to a disproportionate number of people from black and ethnic minority groups being stopped, searched and arrested by the police, and hence having their DNA profiles recorded; it therefore voiced concerns that inferring ethnic identity from biological samples might reinforce racist views of propensity to criminality.

III. RELEVANT NATIONAL AND INTERNATIONAL MATERIALS

A. Council of Europe texts

41. The Council of Europe Convention of 1981 for the protection of individuals with regard to automatic processing of personal data ("the Data Protection Convention"), which entered into force for the United Kingdom on 1 December 1987, defines "personal data" as any information relating to an identified or identifiable individual ("data subject"). The Convention provides, *inter alia*:

Article 5 – Quality of data

"Personal data undergoing automatic processing shall be

...

(b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes;

(c) adequate, relevant and not excessive in relation to the purposes for which they are stored;

...

1. An allele is one of two or more alternative forms of a particular gene. Different alleles may give rise to different forms of the characteristic for which the gene codes (*World Encyclopedia*, Philip's, 2008, Oxford Reference Online: Oxford University Press).

(e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored."

Article 6 – Special categories of data

"Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. ..."

Article 7 – Data security

"Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination."

42. Recommendation No. R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector (adopted on 17 September 1987) states, *inter alia*:

Principle 2 – Collection of data

"2.1. The collection of personal data for police purposes should be limited to such as is necessary for the prevention of a real danger or the suppression of a specific criminal offence. Any exception to this provision should be the subject of specific national legislation.

..."

Principle 3 – Storage of data

"3.1. As far as possible, the storage of personal data for police purposes should be limited to accurate data and to such data as are necessary to allow police bodies to perform their lawful tasks within the framework of national law and their obligations arising from international law.

..."

Principle 7 – Length of storage and updating of data

"7.1. Measures should be taken so that personal data kept for police purposes are deleted if they are no longer necessary for the purposes for which they were stored.

For this purpose, consideration shall in particular be given to the following criteria: the need to retain data in the light of the conclusion of an inquiry into a particular case; a final judicial decision, in particular an acquittal; rehabilitation; spent convictions; amnesties; the age of the data subject, particular categories of data."

43. Recommendation No. R (92) 1 of the Committee of Ministers on the use of analysis of deoxyribonucleic acid (DNA) within the framework of the criminal justice system (adopted on 10 February 1992) states, *inter alia*:

"3. *Use of samples and information derived therefrom*

Samples collected for DNA analysis and the information derived from such analysis for the purpose of the investigation and prosecution of criminal offences must not be used for other purposes. ...

...

Samples taken for DNA analysis and the information so derived may be needed for research and statistical purposes. Such uses are acceptable provided the identity of the individual cannot be ascertained. Names or other identifying references must therefore be removed prior to their use for these purposes.

4. *Taking of samples for DNA analysis*

The taking of samples for DNA analysis should only be carried out in circumstances determined by the domestic law; it being understood that in some states this may necessitate specific authorisation from a judicial authority.

...

8. *Storage of samples and data*

Samples or other body tissue taken from individuals for DNA analysis should not be kept after the rendering of the final decision in the case for which they were used, unless it is necessary for purposes directly linked to those for which they were collected.

Measures should be taken to ensure that the results of DNA analysis are deleted when it is no longer necessary to keep it for the purposes for which it was used. The results of DNA analysis and the information so derived may, however, be retained where the individual concerned has been convicted of serious offences against the life, integrity or security of persons. In such cases strict storage periods should be defined by domestic law.

Samples and other body tissues, or the information derived from them, may be stored for longer periods

– when the person so requests; or

– when the sample cannot be attributed to an individual, for example when it is found at the scene of an offence.

Where the security of the state is involved, the domestic law of the member State may permit retention of the samples, the results of DNA analysis and the information so derived even though the individual concerned has not been charged or convicted of an offence. In such cases strict storage periods should be defined by domestic law.

..."

44. The Explanatory Memorandum to the Recommendation stated, as regards item 8:

"47. The working party was well aware that the drafting of recommendation 8 was a delicate matter, involving different protected interests of a very difficult nature. It was necessary to strike the right balance between these interests. Both the European Convention on Human Rights and the Data Protection Convention provide exceptions for the interests of the suppression of criminal offences and the protection of the rights and freedoms of third parties. However, the exceptions are only allowed to the extent that they are compatible with what is necessary in a democratic society.

...

49. Since the primary aim of the collection of samples and the carrying out of DNA analysis on such samples is the identification of offenders and the exoneration of suspected offenders, the data should be deleted once persons have been cleared of suspicion. The issue then arises as to how long the DNA findings and the samples on which they were based can be stored in the case of a finding of guilt.

50. The general rule should be that the data are deleted when they are no longer necessary for the purposes for which they were collected and used. This would in general be the case when a final decision has been rendered as to the culpability of the offender. By 'final decision' the CAHBI [Ad hoc Committee of Experts on Bioethics] thought that this would normally, under domestic law, refer to a judicial decision. However, the working party recognised that there was a need to set up databases in certain cases and for specific categories of offences which could be considered to constitute circumstances warranting another solution, because of the seriousness of the offences. The working party came to this conclusion after a thorough analysis of the relevant provisions in the European Convention on Human Rights, the Data Protection Convention and other legal instruments drafted within the framework of the Council of Europe. In addition, the working party took into consideration that all member States keep a criminal record and that such record may be used for the purposes of the criminal justice system ... It took into account that such an exception would be permissible under certain strict conditions:

– when there has been a conviction;

– when the conviction concerns a serious criminal offence against the life, integrity and security of a person;

– the storage period is limited strictly;

– the storage is defined and regulated by law;

– the storage is subject to control by Parliament or an independent supervisory body."

B. Law and practice in the Council of Europe member States

45. According to the information provided by the parties or otherwise available to the Court, a majority of the Council of Europe member States allow the compulsory taking of fingerprints and cellular samples in the context of criminal proceedings. At least twenty member States make provision for the taking of DNA information and storing it on national databases or in other forms (Austria, Belgium, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland[1], Italy[2], Latvia, Luxembourg, the Netherlands, Norway, Poland, Spain, Sweden and Switzerland). This number is steadily increasing.

46. In most of these countries (including Austria, Belgium, Finland, France, Germany, Hungary, Ireland, Italy, Luxembourg, the Netherlands, Norway, Poland, Spain and Sweden), the taking of DNA information in the context of criminal proceedings is not systematic but limited to some

1. The law and practice in Ireland are presently governed by the Criminal Justice (Forensic Evidence) Act 1990. A new bill has been approved by the government with a view to extending the use and storage of DNA information in a national database. The bill has not yet been approved by Parliament.

2. The legislative decree of 30 October 2007 establishing a national DNA database was approved by the Italian government and the Senate. However, the decree eventually expired without having been formally converted into a statute as a mistake in the drafting was detected. A corrected version of the decree is expected to be issued in 2008.

specific circumstances and/or to more serious crimes, notably those punishable by certain terms of imprisonment.

47. The United Kingdom is the only member State expressly to permit the systematic and indefinite retention of DNA profiles and cellular samples of persons who have been acquitted or in respect of whom criminal proceedings have been discontinued. Five States (Belgium, Hungary, Ireland, Italy and Sweden) require such information to be destroyed *ex officio* upon acquittal or the discontinuance of the criminal proceedings. Ten other member States apply the same general rule with certain very limited exceptions: Germany, Luxembourg and the Netherlands allow such information to be retained where suspicions remain about the person or if further investigations are needed in a separate case; Austria permits its retention where there is a risk that the suspect will commit a dangerous offence and Poland does likewise in relation to certain serious crimes; Norway and Spain allow the retention of profiles if the defendant is acquitted for lack of criminal accountability; Finland and Denmark allow retention for one and ten years respectively in the event of an acquittal and Switzerland for one year when proceedings have been discontinued. In France, DNA profiles can be retained for twenty-five years after an acquittal or discharge; during this period the public prosecutor may order their earlier deletion, either on his or her own motion or upon request, if their retention has ceased to be required for the purposes of identification in connection with a criminal investigation. Estonia and Latvia also appear to allow the retention of DNA profiles of suspects for certain periods after acquittal.

48. The retention of DNA profiles of convicted persons is allowed, as a general rule, for limited periods of time after the conviction or after the convicted person's death. The United Kingdom thus also appears to be the only member State expressly to allow the systematic and indefinite retention of both profiles and samples of convicted persons.

49. Complaint mechanisms before data-protection monitoring bodies and/or before courts are available in most of the member States with regard to decisions to take cellular samples or retain samples or DNA profiles.

C. European Union

50. Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data provides that the object of national laws on the processing of personal data is notably to protect the right to privacy as recognised both in Article 8 of the European Convention on Human Rights and in the general principles of Community law. The Directive sets out a number of principles in order to give substance to and amplify those contained in the Data Protection Convention of the Council of Europe. It allows member States to adopt legislative measures to restrict the scope of

certain obligations and rights provided for in the Directive when such a restriction constitutes notably a necessary measure for the prevention, investigation, detection and prosecution of criminal offences (Article 13).

51. The Prüm Convention on the stepping up of cross-border cooperation, particularly in combating terrorism, cross-border crime and illegal migration, which was signed by several member States of the European Union on 27 May 2005, sets out rules for the supply of fingerprinting and DNA data to other Contracting Parties and their automated checking against their relevant databases. The Convention provides, *inter alia*:

Article 35 – Purpose

"2. ... The Contracting Party administering the file may process the data supplied ... solely where this is necessary for the purposes of comparison, providing automated replies to searches or recording ... The supplied data shall be deleted immediately following data comparison or automated replies to searches unless further processing is necessary for the purposes mentioned ... above."

52. Article 34 guarantees a level of protection of personal data at least equal to that resulting from the Data Protection Convention and requires the Contracting Parties to take into account Recommendation No. R (87) 15 of the Committee of Ministers of the Council of Europe.

53. The Council framework decision of 24 June 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters states, *inter alia*:

Article 5

"*Establishment of time-limits for erasure and review*

Appropriate time-limits shall be established for the erasure of personal data or for a periodic review of the need for the storage of the data. Procedural measures shall ensure that these time-limits are observed."

D. Case-law in other jurisdictions

54. In the case of *R. v. R.C.* [[2005] 3 SCR 99, 2005 SCC 61] the Supreme Court of Canada considered the issue of retaining a juvenile first-time offender's DNA sample on the national database. The court upheld the decision by a trial judge who had found, in the light of the principles and objects of youth criminal justice legislation, that the impact of the DNA retention would be grossly disproportionate. In his opinion, Fish J observed:

"Of more concern, however, is the impact of an order on an individual's informational privacy interests. In *R. v. Plant*, [1993] 3 S.C.R. 281, at p. 293, the Court found that section 8 of the Charter protected the 'biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state'. An individual's DNA contains the 'highest level of personal and private information': S.A.B., at paragraph 48.

> Unlike a fingerprint, it is capable of revealing the most intimate details of a person's biological make-up. ... The taking and retention of a DNA sample is not a trivial matter and, absent a compelling public interest, would inherently constitute a grave intrusion on the subject's right to personal and informational privacy."

E. United Nations Convention on the Rights of the Child of 1989

55. Article 40 of the United Nations Convention on the Rights of the Child of 20 November 1989 states the right of every child alleged as, accused of, or recognised as having infringed the penal law to be treated in a manner consistent with the promotion of the child's sense of dignity and worth, which reinforces the child's respect for the human rights and fundamental freedoms of others and which takes into account the child's age and the desirability of promoting the child's reintegration and the child's assuming a constructive role in society.

IV. THIRD-PARTY SUBMISSIONS

56. The National Council for Civil Liberties ("Liberty") submitted case-law and scientific material highlighting, *inter alia*, the highly sensitive nature of cellular samples and DNA profiles and the impact on private life arising from their retention by the authorities.

57. Privacy International referred to certain core data-protection rules and principles developed by the Council of Europe and insisted on their high relevance for the interpretation of the proportionality requirement enshrined in Article 8 of the Convention. It emphasised, in particular, the "strict periods" recommended by Recommendation No. R (92) 1 of the Committee of Ministers for the storage of cellular samples and DNA profiles. It further pointed out a disproportionate representation on the United Kingdom National DNA Database of certain groups of the population, notably youth, and the unfairness that that situation might create. The use of data for familial testing and additional research purposes was also of concern. Privacy International also provided a summary of comparative data on the law and practice of different countries with regard to DNA storage and stressed the numerous restrictions and safeguards which existed in that respect.

THE LAW

I. ALLEGED VIOLATION OF ARTICLE 8 OF THE CONVENTION

58. The applicants complained under Article 8 of the Convention about the retention of their fingerprints, cellular samples and DNA profiles pursuant to section 64(1A) of the Police and Criminal Evidence Act 1984 (PACE). Article 8 provides, in so far as relevant, as follows:

> "1. Everyone has the right to respect for his private ... life ...
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society ... for the prevention of disorder or crime ..."

A. Existence of an interference with private life

59. The Court will first consider whether the retention by the authorities of the applicants' fingerprints, DNA profiles and cellular samples constitutes an interference with their private life.

1. The parties' submissions

(a) The applicants

60. The applicants submitted that the retention of their fingerprints, cellular samples and DNA profiles interfered with their right to respect for private life as they were crucially linked to their individual identity and concerned a type of personal information that they were entitled to keep within their control. They pointed out that the initial taking of such bioinformation had consistently been held to engage Article 8 and submitted that their retention was more controversial given the wealth of private information that became permanently available to others and thus came out of the control of the person concerned. They stressed, in particular, the social stigma and psychological implications provoked by such retention in the case of children, which made the interference with the right to private life all the more pressing in respect of the first applicant.

61. They considered that the Convention organs' case-law supported this contention, as did a recent domestic decision of the Information Tribunal (*Chief Constables of West Yorkshire, South Yorkshire and North Wales Police v. the Information Commissioner*, [2005] UK IT EA 2005 0010 (12 October 2005), 173). The latter decision relied on the speech of Baroness Hale of Richmond in the House of Lords (see paragraph 25 above) and followed in substance her finding when deciding a similar question about the application of Article 8 to the retention of conviction data.

62. They further emphasised that the retention of cellular samples involved an even greater degree of interference with Article 8 rights as they contained full genetic information about a person, including genetic information about his or her relatives. It was of no significance whether information was actually extracted from the samples or caused a detriment in a particular case as an individual was entitled to a guarantee that such information, which fundamentally belonged to him, would remain private and not be communicated or accessible without his permission.

(b) The Government

63. The Government accepted that fingerprints, DNA profiles and samples were "personal data" within the meaning of the Data Protection Act in the hands of those who can identify the individual. They considered, however, that the mere retention of fingerprints, DNA profiles and samples for the limited use permitted under section 64 of PACE did not fall within the ambit of the right to respect for private life under Article 8 § 1 of the Convention. Unlike the initial taking of this data, their retention did not interfere with the physical and psychological integrity of the persons; nor did it breach their right to personal development, to establish and develop relationships with other human beings or the right to self-determination.

64. The Government submitted that the applicants' real concerns related to fears about the future uses of stored samples, to anticipated methods of analysis of DNA material and to potential intervention with the private life of individuals through active surveillance. It emphasised in this connection that the permitted extent of the use of the material was clearly and expressly limited by the legislation, the technological processes of DNA profiling and the nature of the DNA profile extracted.

65. The profile was merely a sequence of numbers which provided a means of identifying a person against bodily tissue, containing no materially intrusive information about an individual or his personality. The DNA database was a collection of such profiles which could be searched using material from a crime scene and a person would be identified only if and to the extent that a match was obtained against the sample. Familial searching through partial matches only occurred in very rare cases and was subject to very strict controls. Fingerprints, DNA profiles and samples were neither susceptible to any subjective commentary nor provided any information about a person's activities and thus presented no risk to affect the perception of an individual or affect his or her reputation. Even if such retention were capable of falling within the ambit of Article 8 § 1, the extremely limited nature of any adverse effects rendered the retention not sufficiently serious to constitute an interference.

2. The Court's assessment

(a) General principles

66. The Court notes that the concept of "private life" is a broad term not susceptible to exhaustive definition. It covers the physical and psychological integrity of a person (see *Pretty v. the United Kingdom*, no. 2346/02, § 61, ECHR 2002-III, and *Y.F. v. Turkey*, no. 24209/94, § 33, ECHR 2003-IX). It can therefore embrace multiple aspects of the person's physical and social identity (see *Mikulić v. Croatia*, no. 53176/99, § 53, ECHR 2002-I). Elements such as, for example, gender identification, name and sexual orientation and sexual life fall within the personal sphere protected by Article 8 (see, among other authorities, *Bensaid v. the United Kingdom*, no. 44599/98, § 47, ECHR 2001-I with further references, and *Peck v. the United Kingdom*, no. 44647/98, § 57, ECHR 2003-I). Beyond a person's name, his or her private and family life may include other means of personal identification and of linking to a family (see, *mutatis mutandis*, *Burghartz v. Switzerland*, 22 February 1994, § 24, Series A no. 280-B, and *Ünal Tekeli v. Turkey*, no. 29865/96, § 42, ECHR 2004-X). Information about the person's health is an important element of private life (see *Z v. Finland*, 25 February 1997, § 71, *Reports of Judgments and Decisions* 1997-I). The Court furthermore considers that an individual's ethnic identity must be regarded as another such element (see, in particular, Article 6 of the Data Protection Convention quoted in paragraph 41 above, which lists personal data revealing racial origin as a special category of data along with other sensitive information about an individual). Article 8 protects, in addition, a right to personal development, and the right to establish and develop relationships with other human beings and the outside world (see, for example, *Burghartz*, cited above, opinion of the Commission, p. 37, § 47, and *Friedl v. Austria*, 31 January 1995, Series A no. 305-B, opinion of the Commission, p. 20, § 45). The concept of private life moreover includes elements relating to a person's right to their image (see *Sciacca v. Italy*, no. 50774/99, § 29, ECHR 2005-I).

67. The mere storing of data relating to the private life of an individual amounts to an interference within the meaning of Article 8 (see *Leander v. Sweden*, 26 March 1987, § 48, Series A no. 116). The subsequent use of the stored information has no bearing on that finding (see *Amann v. Switzerland* [GC], no. 27798/95, § 69, ECHR 2000-II). However, in determining whether the personal information retained by the authorities involves any of the private-life aspects mentioned above, the Court will have due regard to the specific context in which the information at issue has been recorded and retained, the nature of the records, the way in which these records are used and processed and the results that may be obtained (see, *mutatis mutandis*, *Friedl*, cited above, §§ 49-51, and *Peck*, cited above, § 59).

(b) Application of the above principles to the present case

68. The Court notes at the outset that all three categories of the personal information retained by the authorities in the present case, namely fingerprints, DNA profiles and cellular samples, constitute personal data within the meaning of the Data Protection Convention as they relate to identified or identifiable individuals. The Government accepted that all three categories are "personal data" within the meaning of the Data Protection Act 1998 in the hands of those who are able to identify the individual.

69. The Convention organs have already considered in various circumstances questions relating to the retention of such personal data by the authorities in the context of criminal proceedings. As regards the nature and scope of the information contained in each of these three categories of data, the Court has distinguished in the past between the retention of fingerprints and the retention of cellular samples and DNA profiles in view of the stronger potential for future use of the personal information contained in the latter (see *Van der Velden v. the Netherlands* (dec.), no. 29514/05, ECHR 2006-XV). The Court considers it appropriate to examine separately the question of interference with the applicants' right to respect for their private lives by the retention of their cellular samples and DNA profiles on the one hand, and of their fingerprints on the other.

(i) Cellular samples and DNA profiles

70. In *Van der Velden*, the Court considered that, given the use to which cellular material in particular could conceivably be put in the future, the systematic retention of that material was sufficiently intrusive to disclose interference with the right to respect for private life (see *Van der Velden*, cited above). The Government criticised that conclusion on the ground that it speculated on the theoretical future use of samples and that there was no such interference at present.

71. The Court maintains its view that an individual's concern about the possible future use of private information retained by the authorities is legitimate and relevant to a determination of the issue of whether there has been an interference. Indeed, bearing in mind the rapid pace of developments in the field of genetics and information technology, the Court cannot discount the possibility that in the future the private-life interests bound up with genetic information may be adversely affected in novel ways or in a manner which cannot be anticipated with precision today. Accordingly, the Court does not find any sufficient reason to depart from its finding in the *Van der Velden* case.

72. Legitimate concerns about the conceivable use of cellular material in the future are not, however, the only element to be taken into account in the determination of the present issue. In addition to the highly personal nature of cellular samples, the Court notes that they contain much sensitive

information about an individual, including information about his or her health. Moreover, samples contain a unique genetic code of great relevance to both the individual and his relatives. In this respect the Court concurs with the opinion expressed by Baroness Hale in the House of Lords (see paragraph 25 above).

73. Given the nature and the amount of personal information contained in cellular samples, their retention *per se* must be regarded as interfering with the right to respect for the private lives of the individuals concerned. That only a limited part of this information is actually extracted or used by the authorities through DNA profiling and that no immediate detriment is caused in a particular case does not change this conclusion (see *Amann*, cited above, § 69).

74. As regards DNA profiles themselves, the Court notes that they contain a more limited amount of personal information extracted from cellular samples in a coded form. The Government submitted that a DNA profile is nothing more than a sequence of numbers or a barcode containing information of a purely objective and irrefutable character and that the identification of a subject only occurs in case of a match with another profile in the database. They also submitted that, being in coded form, computer technology is required to render the information intelligible and that only a limited number of persons would be able to interpret the data in question.

75. The Court observes, nonetheless, that the profiles contain substantial amounts of unique personal data. While the information contained in the profiles may be considered objective and irrefutable in the sense submitted by the Government, their processing through automated means allows the authorities to go well beyond neutral identification. The Court notes in this regard that the Government accepted that DNA profiles could be, and indeed had in some cases been, used for familial searching with a view to identifying a possible genetic relationship between individuals. They also accepted the highly sensitive nature of such searching and the need for very strict controls in this respect. In the Court's view, the DNA profiles' capacity to provide a means of identifying genetic relationships between individuals (see paragraph 39 above) is in itself sufficient to conclude that their retention interferes with the right to the private life of the individuals concerned. The frequency of familial searches, the safeguards attached thereto and the likelihood of detriment in a particular case are immaterial in this respect (see *Amann*, cited above, § 69). This conclusion is similarly not affected by the fact that, since the information is in coded form, it is intelligible only with the use of computer technology and capable of being interpreted only by a limited number of persons.

76. The Court further notes that it is not disputed by the Government that the processing of DNA profiles allows the authorities to assess the likely ethnic origin of the donor and that such techniques are in fact used in

police investigations (see paragraph 40 above). The possibility the DNA profiles create for inferences to be drawn as to ethnic origin makes their retention all the more sensitive and susceptible of affecting the right to private life. This conclusion is consistent with the principle laid down in the Data Protection Convention and reflected in the Data Protection Act that both list personal data revealing ethnic origin among the special categories of sensitive data attracting a heightened level of protection (see paragraphs 30-31 and 41 above).

77. In view of the foregoing, the Court concludes that the retention of both cellular samples and DNA profiles discloses an interference with the applicants' right to respect for their private lives, within the meaning of Article 8 § 1 of the Convention.

(ii) Fingerprints

78. It is common ground that fingerprints do not contain as much information as either cellular samples or DNA profiles. The issue of alleged interference with the right to respect for private life caused by their retention by the authorities has already been considered by the Convention organs.

79. In *McVeigh and Others*, the Commission first examined the issue of the taking and retention of fingerprints as part of a series of investigative measures. It accepted that at least some of the measures disclosed an interference with the applicants' private life, while leaving open the question of whether the retention of fingerprints alone would amount to such interference (see *McVeigh and Others v. the United Kingdom* (nos. 8022/77, 8025/77 and 8027/77, Commission's report of 18 March 1981, Decisions and Reports 25, p. 15, § 224).

80. In *Kinnunen*, the Commission considered that fingerprints and photographs retained following the applicant's arrest did not constitute an interference with his private life as they did not contain any subjective appreciations which called for refutation. The Commission noted, however, that the data at issue had been destroyed nine years later at the applicant's request (see *Kinnunen v. Finland*, no. 24950/94, Commission decision of 15 May 1996, unreported).

81. Having regard to these findings and the questions raised in the present case, the Court considers it appropriate to review this issue. It notes at the outset that the applicants' fingerprint records constitute their personal data (see paragraph 68 above) which contain certain external identification features much in the same way as, for example, personal photographs or voice samples.

82. In *Friedl*, the Commission considered that the retention of anonymous photographs that have been taken at a public demonstration did not interfere with the right to respect for private life. In so deciding, it attached special weight to the fact that the photographs concerned had not been entered in a data-processing system and that the authorities had taken

no steps to identify the persons photographed by means of data processing (see *Friedl*, cited above, §§ 49-51).

83. In *P.G. and J.H. v. the United Kingdom*, the Court considered that the recording of data and the systematic or permanent nature of the record could give rise to private-life considerations even though the data in question may have been available in the public domain or otherwise. The Court noted that a permanent record of a person's voice for further analysis was of direct relevance to identifying that person when considered in conjunction with other personal data. It accordingly regarded the recording of the applicants' voices for such further analysis as amounting to interference with their right to respect for their private lives (see *P.G. and J.H. v. the United Kingdom*, no. 44787/98, §§ 59-60, ECHR 2001-IX).

84. The Court is of the view that the general approach taken by the Convention organs in respect of photographs and voice samples should also be followed in respect of fingerprints. The Government distinguished the latter by arguing that they constituted neutral, objective and irrefutable material and, unlike photographs, were unintelligible to the untutored eye and without a comparator fingerprint. While true, this consideration cannot alter the fact that fingerprints objectively contain unique information about the individual concerned, allowing his or her identification with precision in a wide range of circumstances. They are thus capable of affecting his or her private life and the retention of this information without the consent of the individual concerned cannot be regarded as neutral or insignificant.

85. The Court accordingly considers that the retention of fingerprints on the authorities' records in connection with an identified or identifiable individual may in itself give rise, notwithstanding their objective and irrefutable character, to important private-life concerns.

86. In the instant case, the Court notes furthermore that the applicants' fingerprints were initially taken in criminal proceedings and subsequently recorded on a national database with the aim of being permanently kept and regularly processed by automated means for criminal-identification purposes. It is accepted in this regard that, because of the information they contain, the retention of cellular samples and DNA profiles has a more important impact on private life than the retention of fingerprints. However, the Court, like Baroness Hale (see paragraph 25 above), considers that, while it may be necessary to distinguish between the taking, use and storage of fingerprints, on the one hand, and samples and profiles, on the other, in determining the question of justification, the retention of fingerprints constitutes an interference with the right to respect for private life.

172

B. Justification for the interference

1. The parties' submissions

(a) The applicants

87. The applicants argued that the retention of fingerprints, cellular samples and DNA profiles was not justified under Article 8 § 2. The Government were given a very wide remit to use samples and DNA profiles notably for "purposes related to the prevention or detection of crime", "the investigation of an offence" or "the conduct of a prosecution". These purposes were vague and open to abuse as they might, in particular, lead to the collation of detailed personal information outside the immediate context of the investigation of a particular offence. The applicants further submitted that there were insufficient procedural safeguards against misuse or abuse of the information. Records on the Police National Computer (PNC) were not only accessible to the police, but also to fifty-six non-police bodies, including government agencies and departments, private groups such as British Telecom and the Association of British Insurers, and even certain employers. Furthermore, the PNC was linked to the Europe-wide "Schengen Information System". Consequently, their case involved a very substantial and controversial interference with the right to private life, as notably illustrated by ongoing public debate and disagreement about the subject in the United Kingdom. Contrary to the assertion of the Government, the applicants concluded that the issue of the retention of this material was of great individual concern and the State had a narrow margin of appreciation in this field.

88. The applicants contended that the indefinite retention of fingerprints, cellular samples and DNA profiles of unconvicted persons could not be regarded as "necessary in a democratic society" for the purpose of preventing crime. In particular, there was no justification at all for the retention of cellular samples following the original generation of the DNA profile; nor had the efficacy of the profiles' retention been convincingly demonstrated since the high number of DNA matches relied upon by the Government was not shown to have led to successful prosecutions. Likewise, in most of the specific examples provided by the Government, the successful prosecution had not been contingent on the retention of the records and in certain others the successful outcome could have been achieved through more limited retention in time and scope.

89. The applicants further submitted that the retention was disproportionate because of its blanket nature irrespective of the offences involved, the unlimited period, the failure to take account of the applicants' circumstances and the lack of an independent decision-making process or scrutiny when considering whether or not to order retention. They further considered the retention regime to be inconsistent with the Council of

Europe's guidance on the subject. They emphasised, finally, that retention of the records cast suspicion on persons who had been acquitted or discharged of crimes, thus implying that they were not wholly innocent. The retention thus resulted in stigma which was particularly detrimental to children, as in the case of S., and to members of certain ethnic groups over-represented on the database.

(b) The Government

90. The Government submitted that any interference resulting from the retention of the applicants' fingerprints, cellular samples and DNA profiles was justified under Article 8 § 2. It was in accordance with the law as expressly provided for, and governed by section 64 of PACE, which set out detailed powers and restrictions on the taking of fingerprints and samples and clearly stated that they would be retained by the authorities regardless of the outcome of the proceedings in respect of which they were taken. The exercise of the discretion to retain fingerprints and samples was also, in any event, subject to the normal principles of law regulating discretionary power and to judicial review.

91. The Government further stated that the interference was necessary and proportionate for the legitimate purpose of the prevention of disorder or crime and/or the protection of the rights and freedoms of others. It was of vital importance that law enforcement agencies took full advantage of available techniques of modern technology and forensic science in the prevention, investigation and detection of crime for the interests of society generally. They submitted that the retained material was of inestimable value in the fight against crime and terrorism and the detection of the guilty, and provided statistics in support of this view. They emphasised that the benefits to the criminal-justice system were enormous, not only permitting the detection of the guilty but also eliminating the innocent from inquiries and correcting and preventing miscarriages of justice.

92. As at 30 September 2005, the National DNA Database held 181,000 profiles from individuals who would have been entitled to have those profiles destroyed before the 2001 amendments. Of those profiles, 8,251 were subsequently linked with crime-scene stains which involved 13,079 offences, including 109 murders, 55 attempted murders, 116 rapes, 67 sexual offences, 105 aggravated burglaries and 126 offences of the supply of controlled drugs.

93. The Government also submitted specific examples of the use of DNA material for successful investigation and prosecution in some eighteen specific cases. In ten of these cases the DNA profiles of suspects matched some earlier unrelated crime-scene stains retained on the database, thus allowing successful prosecution for those earlier crimes. In another case, two suspects arrested for rape were eliminated from the investigation as their DNA profiles did not match the crime-scene stain. In two other cases

the retention of DNA profiles of the persons found guilty of certain minor offences (disorder and theft) led to establishing their involvement in other crimes committed later. In one case the retention of a suspect's DNA profile following an alleged immigration offence helped his extradition to the United Kingdom a year later when he was identified by one of his victims as having committed rape and murder. Finally, in four cases DNA profiles retained from four persons suspected but not convicted of certain offences (possession of offensive weapons, violent disorder and assault) matched the crime-scene stains collected from victims of rape up to two years later.

94. The Government contended that the retention of fingerprints, cellular samples and DNA profiles could not be regarded as excessive since they were kept for specific limited statutory purposes and stored securely and subject to the safeguards identified. Their retention was neither warranted by any degree of suspicion of the applicants' involvement in a crime or propensity to crime nor directed at retaining records in respect of investigated alleged offences in the past. The records were retained because the police had already been lawfully in possession of them, and their retention would assist in the future prevention and detection of crime in general by increasing the size of the database. Retention resulted in no stigma and produced no practical consequence for the applicants unless the records matched a crime-scene profile. A fair balance was thus struck between individual rights and the general interest of the community and fell within the State's margin of appreciation.

2. The Court's assessment

(a) In accordance with the law

95. The Court notes from its well established case-law that the wording "in accordance with the law" requires the impugned measure both to have some basis in domestic law and to be compatible with the rule of law, which is expressly mentioned in the Preamble to the Convention and inherent in the object and purpose of Article 8. The law must thus be adequately accessible and foreseeable, that is, formulated with sufficient precision to enable the individual – if need be with appropriate advice – to regulate his conduct. For domestic law to meet these requirements, it must afford adequate legal protection against arbitrariness and accordingly indicate with sufficient clarity the scope of discretion conferred on the competent authorities and the manner of its exercise (see *Malone v. the United Kingdom*, 2 August 1984, §§ 66-68, Series A no. 82; *Rotaru v. Romania* [GC], no. 28341/95, § 55, ECHR 2000-V; and *Amann*, cited above, § 56).

96. The level of precision required of domestic legislation – which cannot in any case provide for every eventuality – depends to a considerable degree on the content of the instrument in question, the field it is designed to cover and the number and status of those to whom it is addressed (see

Hasan and Chaush v. Bulgaria [GC], no. 30985/96, § 84, ECHR 2000-XI, with further references).

97. The Court notes that section 64 of PACE provides that the fingerprints or samples taken from a person in connection with the investigation of an offence may be retained after they have fulfilled the purposes for which they were taken (see paragraph 27 above). The Court agrees with the Government that the retention of the applicants' fingerprint and DNA records had a clear basis in the domestic law. There is also clear evidence that these records are retained in practice save in exceptional circumstances. The fact that chief police officers have power to destroy them in such rare cases does not make the law insufficiently certain from the point of view of the Convention.

98. As regards the conditions attached to and arrangements for the storing and use of this personal information, section 64 is far less precise. It provides that retained samples and fingerprints must not be used by any person except for purposes related to the prevention or detection of crime, the investigation of an offence or the conduct of a prosecution.

99. The Court agrees with the applicants that at least the first of these purposes is worded in rather general terms and may give rise to extensive interpretation. It reiterates that it is as essential, in this context, as in telephone tapping, secret surveillance and covert intelligence-gathering, to have clear, detailed rules governing the scope and application of measures, as well as minimum safeguards concerning, *inter alia*, duration, storage, usage, access of third parties, procedures for preserving the integrity and confidentiality of data and procedures for its destruction, thus providing sufficient guarantees against the risk of abuse and arbitrariness (see, *mutatis mutandis*, *Kruslin v. France*, 24 April 1990, §§ 33 and 35, Series A no. 176-A; *Rotaru*, cited above, §§ 57-59; *Weber and Saravia v. Germany* (dec.), no. 54934/00, ECHR 2006-XI; *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria*, no. 62540/00, §§ 75-77, 28 June 2007; and *Liberty and Others v. the United Kingdom*, no. 58243/00, §§ 62-63, 1 July 2008). The Court notes, however, that these questions are in this case closely related to the broader issue of whether the interference was necessary in a democratic society. In view of its analysis in paragraphs 105-26 below, the Court does not find it necessary to decide whether the wording of section 64 meets the "quality of law" requirements within the meaning of Article 8 § 2 of the Convention.

(b) Legitimate aim

100. The Court agrees with the Government that the retention of fingerprint and DNA information pursues the legitimate purpose of the detection and, therefore, prevention of crime. While the original taking of this information pursues the aim of linking a particular person to the

particular crime of which he or she is suspected, its retention pursues the broader purpose of assisting in the identification of future offenders.

(c) Necessary in a democratic society

(i) General principles

101. An interference will be considered "necessary in a democratic society" for a legitimate aim if it answers a "pressing social need" and, in particular, if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are "relevant and sufficient". While it is for the national authorities to make the initial assessment in all these respects, the final evaluation of whether the interference is necessary remains subject to review by the Court for conformity with the requirements of the Convention (see *Coster v. the United Kingdom* [GC], no. 24876/94, § 104, 18 January 2001, with further references).

102. A margin of appreciation must be left to the competent national authorities in this assessment. The breadth of this margin varies and depends on a number of factors, including the nature of the Convention right in issue, its importance for the individual, the nature of the interference and the object pursued by the interference. The margin will tend to be narrower where the right at stake is crucial to the individual's effective enjoyment of intimate or key rights (see *Connors v. the United Kingdom*, no. 66746/01, § 82, 27 May 2004, with further references). Where a particularly important facet of an individual's existence or identity is at stake, the margin allowed to the State will be restricted (see *Evans v. the United Kingdom* [GC], no. 6339/05, § 77, ECHR 2007-I). Where, however, there is no consensus within the member States of the Council of Europe, either as to the relative importance of the interest at stake or as to how best to protect it, the margin will be wider (see *Dickson v. the United Kingdom* [GC], no. 44362/04, § 78, ECHR 2007-V).

103. The protection of personal data is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life, as guaranteed by Article 8 of the Convention. The domestic law must afford appropriate safeguards to prevent any such use of personal data as may be inconsistent with the guarantees of this Article (see, *mutatis mutandis*, *Z v. Finland*, cited above, § 95). The need for such safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned, not least when such data are used for police purposes. The domestic law should notably ensure that such data are relevant and not excessive in relation to the purposes for which they are stored; and preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored (see Article 5 of the Data Protection Convention and the Preamble thereto and

Principle 7 of Recommendation No. R (87) 15 of the Committee of Ministers regulating the use of personal data in the police sector). The domestic law must also afford adequate guarantees that retained personal data were efficiently protected from misuse and abuse (see notably Article 7 of the Data Protection Convention). The above considerations are especially valid as regards the protection of special categories of more sensitive data (see Article 6 of the Data Protection Convention) and more particularly of DNA information, which contains the person's genetic make-up of great importance to both the person concerned and his or her family (see Recommendation No. R (92) 1 of the Committee of Ministers on the use of analysis of DNA within the framework of the criminal justice system).

104. The interests of the data subjects and the community as a whole in protecting the personal data, including fingerprint and DNA information, may be outweighed by the legitimate interest in the prevention of crime (see Article 9 of the Data Protection Convention). However, the intrinsically private character of this information calls for the Court to exercise careful scrutiny of any State measure authorising its retention and use by the authorities without the consent of the person concerned (see, *mutatis mutandis*, *Z v. Finland*, cited above, § 96).

(ii) Application of these principles to the present case

105. The Court finds it to be beyond dispute that the fight against crime, and in particular against organised crime and terrorism, which is one of the challenges faced by today's European societies, depends to a great extent on the use of modern scientific techniques of investigation and identification. The techniques of DNA analysis were acknowledged by the Council of Europe more than fifteen years ago as offering advantages to the criminal-justice system (see Recommendation No. R (92) 1 of the Committee of Ministers, paragraphs 43-44 above). Nor is it disputed that the member States have since that time made rapid and marked progress in using DNA information in the determination of innocence or guilt.

106. However, while it recognises the importance of such information in the detection of crime, the Court must delimit the scope of its examination. The question is not whether the retention of fingerprints, cellular samples and DNA profiles may in general be regarded as justified under the Convention. The only issue to be considered by the Court is whether the retention of the fingerprint and DNA data of the applicants, as persons who had been suspected, but not convicted, of certain criminal offences, was justified under Article 8 § 2 of the Convention.

107. The Court will consider this issue with due regard to the relevant instruments of the Council of Europe and the law and practice of the other Contracting States. The core principles of data protection require the retention of data to be proportionate in relation to the purpose of collection and insist on limited periods of storage (see paragraphs 41-44 above). These

principles appear to have been consistently applied by the Contracting States in the police sector in accordance with the Data Protection Convention and subsequent Recommendations of the Committee of Ministers (see paragraphs 45-49 above).

108. As regards, more particularly, cellular samples, most of the Contracting States allow these materials to be taken in criminal proceedings only from individuals suspected of having committed offences of a certain minimum gravity. In the great majority of the Contracting States with functioning DNA databases, samples and DNA profiles derived from those samples are required to be removed or destroyed either immediately or within a certain limited time after acquittal or discharge. A restricted number of exceptions to this principle are allowed by some Contracting States (see paragraphs 47-48 above).

109. The current position of Scotland, as a part of the United Kingdom itself, is of particular significance in this regard. As noted above (see paragraph 36), the Scottish parliament voted to allow retention of the DNA of unconvicted persons only in the case of adults charged with violent or sexual offences and even then, for three years only, with the possibility of an extension to keep the DNA sample and data for a further two years with the consent of a sheriff.

110. This position is notably consistent with Recommendation No. R (92) 1 of the Committee of Ministers, which stresses the need for an approach which discriminates between different kinds of cases and for the application of strictly defined storage periods for data, even in more serious cases (see paragraphs 43-44 above). Against this background, England, Wales and Northern Ireland appear to be the only jurisdictions within the Council of Europe to allow the indefinite retention of fingerprint and DNA material of any person of any age suspected of any recordable offence.

111. The Government lay emphasis on the fact that the United Kingdom is in the vanguard of the development of the use of DNA samples in the detection of crime and that other States have not yet achieved the same maturity in terms of the size and resources of DNA databases. It is argued that the comparative analysis of the law and practice in other States with less advanced systems is accordingly of limited importance.

112. The Court cannot, however, disregard the fact that, notwithstanding the advantages provided by comprehensive extension of the DNA database, other Contracting States have chosen to set limits on the retention and use of such data with a view to achieving a proper balance with the competing interests of preserving respect for private life. The Court observes that the protection afforded by Article 8 of the Convention would be unacceptably weakened if the use of modern scientific techniques in the criminal-justice system were allowed at any cost and without carefully balancing the potential benefits of the extensive use of such techniques against important private-life interests. In the Court's view, the strong consensus existing

among the Contracting States in this respect is of considerable importance and narrows the margin of appreciation left to the respondent State in the assessment of the permissible limits of the interference with private life in this sphere. The Court considers that any State claiming a pioneer role in the development of new technologies bears special responsibility for striking the right balance in this regard.

113. In the present case, the applicants' fingerprints and cellular samples were taken and DNA profiles obtained in the context of criminal proceedings brought on suspicion of attempted robbery in the case of the first applicant and harassment of his partner in the case of the second applicant. The data were retained on the basis of legislation allowing for their indefinite retention, despite the acquittal of the former and the discontinuance of the criminal proceedings against the latter.

114. The Court must consider whether the permanent retention of fingerprint and DNA data of all suspected but unconvicted people is based on relevant and sufficient reasons.

115. Although the power to retain fingerprints, cellular samples and DNA profiles of unconvicted persons has only existed in England and Wales since 2001, the Government argue that their retention has been shown to be indispensable in the fight against crime. Certainly, the statistical and other evidence, which was before the House of Lords and is included in the material supplied by the Government (see paragraph 92 above) appears impressive, indicating that DNA profiles that would have been previously destroyed were linked with crime-scene stains in a high number of cases.

116. The applicants, however, assert that the statistics are misleading, a view supported in the Nuffield Council on Bioethics' report. It is true, as pointed out by the applicants, that the figures do not reveal the extent to which this "link" with crime scenes resulted in convictions of the persons concerned or the number of convictions that were contingent on the retention of the samples of unconvicted persons. Nor do they demonstrate that the high number of successful matches with crime-scene stains was only made possible through indefinite retention of DNA records of all such persons. At the same time, in the majority of the specific cases quoted by the Government (see paragraph 93 above), the DNA records taken from the suspects produced successful matches only with earlier crime-scene stains retained on the database. Yet such matches could have been made even in the absence of the present scheme, which permits the indefinite retention of DNA records of all suspected but unconvicted persons.

117. While neither the statistics nor the examples provided by the Government in themselves establish that the successful identification and prosecution of offenders could not have been achieved without the permanent and indiscriminate retention of the fingerprint and DNA records of all persons in the applicants' position, the Court accepts that the

extension of the database has nonetheless contributed to the detection and prevention of crime.

118. The question, however, remains whether such retention is proportionate and strikes a fair balance between the competing public and private interests.

119. In this respect, the Court is struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken – and retained – from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time-limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the national database or the materials destroyed (see paragraph 35 above); in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances.

120. The Court acknowledges that the level of interference with the applicants' right to private life may be different for each of the three different categories of personal data retained. The retention of cellular samples is particularly intrusive given the wealth of genetic and health information contained therein. However, such an indiscriminate and open-ended retention regime as the one in issue calls for careful scrutiny regardless of these differences.

121. The Government contend that the retention could not be considered as having any direct or significant effect on the applicants unless matches in the database were to implicate them in the commission of offences on a future occasion. The Court is unable to accept this argument and reiterates that the mere retention and storing of personal data by public authorities, however obtained, are to be regarded as having a direct impact on the private-life interest of an individual concerned, irrespective of whether subsequent use is made of the data (see paragraph 67 above).

122. Of particular concern in the present context is the risk of stigmatisation, stemming from the fact that persons in the position of the applicants, who have not been convicted of any offence and are entitled to the presumption of innocence, are treated in the same way as convicted persons. In this respect, the Court must bear in mind that the right of every person under the Convention to be presumed innocent includes the general rule that no suspicion regarding an accused's innocence may be voiced after his acquittal (see *Rushiti v. Austria*, no. 28389/95, § 31, 21 March 2000, with further references). It is true that the retention of the applicants' private

data cannot be equated with the voicing of suspicions. Nonetheless, their perception that they are not being treated as innocent is heightened by the fact that their data are retained indefinitely in the same way as the data of convicted persons, while the data of those who have never been suspected of an offence are required to be destroyed.

123. The Government argue that the power of retention applies to all fingerprints and samples taken from a person in connection with the investigation of an offence and does not depend on innocence or guilt. It is further submitted that the fingerprints and samples have been lawfully taken and that their retention is not related to the fact that they were originally suspected of committing a crime, the sole reason for their retention being to increase the size and, therefore, the use of the database in the identification of offenders in the future. The Court, however, finds this argument difficult to reconcile with the obligation imposed by section 64(3) of PACE to destroy the fingerprints and samples of volunteers at their request, despite the similar value of the material in increasing the size and utility of the database. Weighty reasons would have to be put forward by the Government before the Court could regard as justified such a difference in treatment of the applicants' private data compared to that of other unconvicted people.

124. The Court further considers that the retention of the unconvicted persons' data may be especially harmful in the case of minors such as the first applicant, given their special situation and the importance of their development and integration in society. The Court has already emphasised, drawing on the provisions of Article 40 of the United Nations Convention on the Rights of the Child of 1989, the special position of minors in the criminal-justice sphere and has noted, in particular, the need for the protection of their privacy at criminal trials (see *T. v. the United Kingdom* [GC], no. 24724/94, §§ 75 and 85, 16 December 1999). In the same way, the Court considers that particular attention should be paid to the protection of juveniles from any detriment that may result from the retention by the authorities of their private data following acquittals of a criminal offence. The Court shares the view of the Nuffield Council on Bioethics as to the impact on young persons of the indefinite retention of their DNA material and notes the Council's concerns that the policies applied have led to the over-representation in the database of young persons and ethnic minorities who have not been convicted of any crime (see paragraphs 38-40 above).

125. In conclusion, the Court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent State has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot

be regarded as necessary in a democratic society. This conclusion obviates the need for the Court to consider the applicants' criticism regarding the adequacy of certain particular safeguards, such as too broad an access to the personal data concerned and insufficient protection against the misuse or abuse of such data.

126. Accordingly, there has been a violation of Article 8 of the Convention in the present case.

II. ALLEGED VIOLATION OF ARTICLE 14 TAKEN TOGETHER WITH ARTICLE 8 OF THE CONVENTION

127. The applicants submitted that they had been subjected to discriminatory treatment as compared to others in an analogous situation, namely other unconvicted persons whose samples had still to be destroyed under the legislation. This treatment related to their status and fell within the ambit of Article 14 of the Convention, which had always been liberally interpreted. For the reasons set out in their submissions under Article 8, there was no reasonable or objective justification for the treatment, nor any legitimate aim or reasonable relationship of proportionality to the purported aim of crime prevention, in particular as regards the samples which played no role in crime detection or prevention. It was an entirely improper and prejudicial differentiation to retain materials of persons who should be presumed to be innocent.

128. The Government submitted that as Article 8 was not engaged, Article 14 of the Convention was not applicable. Even if it were, there was no difference of treatment as all those in an analogous situation to the applicants were treated the same and the applicants could not compare themselves with those who had not had samples taken by the police or those who consented to give samples voluntarily. In any event, any difference in treatment complained of was not based on "status" or a personal characteristic but on historical fact. If there was any difference in treatment, it was objectively justified and within the State's margin of appreciation.

129. The Court refers to its conclusion above that the retention of the applicants' fingerprints, cellular samples and DNA profiles was in violation of Article 8 of the Convention. In the light of the reasoning that has led to this conclusion, the Court considers that it is not necessary to examine separately the applicants' complaint under Article 14 of the Convention.

III. APPLICATION OF ARTICLE 41 OF THE CONVENTION

130. Article 41 of the Convention provides:

> "If the Court finds that there has been a violation of the Convention or the Protocols thereto, and if the internal law of the High Contracting Party concerned allows only partial reparation to be made, the Court shall, if necessary, afford just satisfaction to the injured party."

131. The applicants requested the Court to award them just satisfaction for non-pecuniary damage and for costs and expenses.

A. Non-pecuniary damage

132. The applicants claimed compensation for non-pecuniary damage in the sum of 5,000 pounds sterling (GBP) each for distress and anxiety caused by the knowledge that intimate information about each of them had been unjustifiably retained by the State, and in relation to anxiety and stress caused by the need to pursue this matter through the courts.

133. The Government, referring to the Court's case-law (see, in particular, *Amann v. Switzerland* [GC], no. 27798/95, ECHR 2000-II), submitted that a finding of a violation would in itself constitute sufficient just satisfaction for both applicants and distinguished the present case from those cases where violations had been found as a result of the use or disclosure of the personal information (see, in particular, *Rotaru v. Romania* [GC], no. 28341/95, ECHR 2000-V).

134. The Court notes that it has found that the retention of the applicants' fingerprint and DNA data violates their rights under Article 8 of the Convention. In accordance with Article 46 of the Convention, it will be for the respondent State to implement, under the supervision of the Committee of Ministers, appropriate general and/or individual measures to fulfil its obligations to secure the right of the applicants and other persons in their position to respect for their private life (see *Scozzari and Giunta v. Italy* [GC], nos. 39221/98 and 41963/98, § 249, ECHR 2000-VIII, and *Christine Goodwin v. the United Kingdom* [GC], no. 28957/95, § 120, ECHR 2002-VI). In these circumstances, the Court considers that the finding of a violation, with the consequences which will ensue for the future, may be regarded as constituting sufficient just satisfaction in this respect. The Court accordingly rejects the applicants' claim for non-pecuniary damage.

B. Costs and expenses

135. The applicants also requested the Court to award GBP 52,066.25 for costs and expenses incurred before the Court and attached detailed documentation in support of their claim. These included the costs of the

solicitor (GBP 15,083.12) and the fees of three counsel (GBP 21,267.50, GBP 2,937.50 and GBP 12,778.13 respectively). The hourly rates charged by the lawyers were as follows: GBP 140 in respect of the applicants' solicitor (increased to GBP 183 as from June 2007) and GBP 150, GBP 250 and GBP 125 respectively in respect of three counsel.

136. The Government qualified the applicants' claim as entirely unreasonable. They submitted in particular that the rates charged by the lawyers were excessive and should be reduced to no more than two-thirds of the level claimed. They also argued that no award should be made in respect of the applicants' decision to instruct a fourth lawyer at a late stage of the proceedings as it had led to the duplication of work. The Government concluded that any cost award should be limited to GBP 15,000 and in any event, to no more than GBP 20,000.

137. The Court reiterates that only legal costs and expenses found to have been actually and necessarily incurred and which are reasonable as to quantum are recoverable under Article 41 of the Convention (see, among other authorities, *Roche v. the United Kingdom* [GC], no. 32555/96, § 182, ECHR 2005-X).

138. On the one hand, the present applications were of some complexity as they required examination in a Chamber and in the Grand Chamber, including several rounds of observations and an oral hearing. The application also raised important legal issues and questions of principle requiring a large amount of work. It notably required an in-depth examination of the current debate on the issue of retention of fingerprint and DNA records in the United Kingdom and a comprehensive comparative research of the law and practice of other Contracting States and of the relevant texts and documents of the Council of Europe.

139. On the other hand, the Court considers that the overall sum of GBP 52,066.25 claimed by the applicants is excessive as to quantum. In particular, the Court agrees with the Government that the appointment of the fourth lawyer in the later stages of the proceedings may have led to a certain amount of duplication of work.

140. Making its assessment on an equitable basis and in the light of its practice in comparable cases, the Court awards the sum of 42,000 euros (EUR) in respect of costs and expenses, less the amount of EUR 2,613.07 already paid by the Council of Europe in legal aid.

C. Default interest

141. The Court considers it appropriate that the default interest rate should be based on the marginal lending rate of the European Central Bank, to which should be added three percentage points.

FOR THESE REASONS, THE COURT UNANIMOUSLY

1. *Holds* that there has been a violation of Article 8 of the Convention;

2. *Holds* that it is not necessary to examine separately the complaint under Article 14 of the Convention;

3. *Holds* that the finding of a violation constitutes in itself sufficient just satisfaction for the non-pecuniary damage sustained by the applicants;

4. *Holds*
(a) that the respondent State is to pay the applicants, within three months, EUR 42,000 (forty-two thousand euros) in respect of costs and expenses (inclusive of any tax which may be chargeable to the applicants), to be converted into pounds sterling at the rate applicable at the date of settlement, less EUR 2,613.07 already paid to the applicants in respect of legal aid;
(b) that from the expiry of the above-mentioned three months until settlement simple interest shall be payable on the above amount at a rate equal to the marginal lending rate of the European Central Bank during the default period plus three percentage points;

5. *Dismisses* the remainder of the applicants' claim for just satisfaction.

Done in English and in French, and delivered at a public hearing in the Human Rights Building, Strasbourg, on 4 December 2008.

Michael O'Boyle
Deputy Registrar

Jean-Paul Costa
President

615 F.3d 263, 38 Media L. Rep. 2442
(Cite as: 615 F.3d 263)

H

United States Court of Appeals,
Fourth Circuit.
Betty J. OSTERGREN, Plaintiff–Appellee,
v.
Kenneth T. CUCCINELLI, II, in his official capacity as Attorney General of Virginia, Defendant–Appellant.
Electronic Privacy Information Center, Amicus Supporting Appellee.
Betty J. Ostergren, Plaintiff–Appellant,
v.
Kenneth T. Cuccinelli, II, in his official capacity as Attorney General of Virginia, Defendant–Appellee.
Electronic Privacy Information Center, Amicus Supporting Appellant.

Nos. 09–1723, 09–1796.
Argued: March 23, 2010.
Decided: July 26, 2010.

Background: Privacy advocate brought action challenging Virginia's Personal Information Privacy Act on First Amendment grounds, as applied to advocate's website that criticized state's release of private information and showed publicly-available Virginia land records that contained unredacted Social Security numbers (SSNs). The United States District Court for the Eastern District of Virginia, Robert E. Payne, Senior District Judge, 2008 WL 3895593, found unconstitutional a section of the Act prohibiting intentional communication of another individual's SSN, and, 643 F.Supp.2d 758, issued permanent injunction barring state from punishing republication of publicly-available land records, including unredacted SSNs, for various state legislators, executive officers, and clerks of court in effort to reform law. Parties appealed.

Holdings: The Court of Appeals, Duncan, Circuit Judge, held that:
(1) advocate's publication of records containing unredacted SSNs was protected by First Amendment;
(2) Virginia's failure to redact SSNs before posting records online meant that statute was not narrowly tailored to Virginia's interest in protecting individual privacy;
(3) court lacked jurisdiction, on injunction motion, to answer question as to whether First Amendment prohibited enforcement of statute as to records from other states; and
(4) injunction was not properly tailored to fit nature and extent of First Amendment violation.

Affirmed in part and reversed and remanded in part.

Davis, Circuit Judge, concurred and filed opinion.

West Headnotes

[1] Constitutional Law 92 ⇐1518

92 Constitutional Law
92XVIII Freedom of Speech, Expression, and Press
92XVIII(A) In General
92XVIII(A)1 In General
92k1516 Content-Based Regulations or Restrictions
92k1518 k. Strict or exacting scrutiny; compelling interest test. Most Cited Cases

Laws restricting the content of expression normally are invalid under the First Amendment unless narrowly tailored to promote a compelling state interest. U.S.C.A. Const.Amend. 1.

[2] Constitutional Law 92 ⇐1562

92 Constitutional Law
92XVIII Freedom of Speech, Expression, and Press
92XVIII(A) In General
92XVIII(A)3 Particular Issues and Applications in General
92k1562 k. "Fighting words". Most

Cited Cases

Constitutional Law 92 ⚿1801

92 Constitutional Law
92XVIII Freedom of Speech, Expression, and Press
92XVIII(H) Law Enforcement; Criminal Conduct
92k1801 k. Incitement or encouragement of crime or lawless action. Most Cited Cases

Constitutional Law 92 ⚿2191

92 Constitutional Law
92XVIII Freedom of Speech, Expression, and Press
92XVIII(Y) Sexual Expression
92k2189 Obscenity in General
92k2191 k. Lack of constitutional protection. Most Cited Cases

Constitutional Law 92 ⚿2246

92 Constitutional Law
92XVIII Freedom of Speech, Expression, and Press
92XVIII(Y) Sexual Expression
92k2244 Children and Minors, Protection of
92k2246 k. Pornography. Most Cited Cases

Fighting words, obscenity, incitement of illegal activity, and child pornography are examples of unprotected speech that may be circumscribed entirely because these categories of speech are not an essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality. U.S.C.A. Const.Amend. 1.

[3] Constitutional Law 92 ⚿1570

92 Constitutional Law
92XVIII Freedom of Speech, Expression, and Press
92XVIII(A) In General
92XVIII(A)3 Particular Issues and Applications in General
92k1570 k. Government records. Most Cited Cases

Records 326 ⚿31

326 Records
326II Public Access
326II(A) In General
326k31 k. Regulations limiting access; offenses. Most Cited Cases

Privacy advocate's publication of Virginia land records containing unredacted Social Security numbers (SSNs) was protected by First Amendment; advocate communicated SSNs, not by listing them beside people's names, but rather by providing copies of entire documents maintained by government officials, thereby drawing attention to state's failure to safeguard private information and powerfully demonstrating why Virginia citizens should be concerned. U.S.C.A. Const.Amend. 1.

[4] Constitutional Law 92 ⚿1490

92 Constitutional Law
92XVIII Freedom of Speech, Expression, and Press
92XVIII(A) In General
92XVIII(A)1 In General
92k1490 k. In general. Most Cited Cases

One party's freedom of speech must be weighed against others' right of privacy. U.S.C.A. Const.Amend. 1.

[5] Constitutional Law 92 ⚿1506

92 Constitutional Law
92XVIII Freedom of Speech, Expression, and Press
92XVIII(A) In General
92XVIII(A)1 In General
92k1506 k. Strict or exacting scrutiny; compelling interest test. Most Cited Cases

In deciding what constitutes a state interest of the highest order, so as to warrant a state's regulation of speech, courts cannot be bound by the state's view and its conduct. U.S.C.A. Const.Amend. 1.

[6] Constitutional Law 92 ⇐1506

92 Constitutional Law
92XVIII Freedom of Speech, Expression, and Press
92XVIII(A) In General
92XVIII(A)1 In General
92k1506 k. Strict or exacting scrutiny; compelling interest test. Most Cited Cases

Objective criteria can be considered when deciding what constitutes a state interest of the highest order, so as to warrant a state's regulation of speech. U.S.C.A. Const.Amend. 1.

[7] Records 326 ⇐31

326 Records
326II Public Access
326II(A) In General
326k31 k. Regulations limiting access; offenses. Most Cited Cases

Individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form.

[8] Constitutional Law 92 ⇐2151

92 Constitutional Law
92XVIII Freedom of Speech, Expression, and Press
92XVIII(W) Telecommunications and Computers
92k2148 Internet
92k2151 k. Website content. Most Cited Cases

Records 326 ⇐31

326 Records
326II Public Access
326II(A) In General
326k31 k. Regulations limiting access; offenses. Most Cited Cases

Virginia's failure to redact Social Security numbers (SSNs) before placing land records online meant that statute, which barred intentional communication of another person's SSN, was not narrowly tailored to Virginia's interest in protecting individual privacy, and thus applying statute to punish privacy advocate's protected speech of posting those records, with unredacted SSNs, on her website in effort to draw attention to state's failure to protect citizens' privacy interests violated advocate's First Amendment rights. U.S.C.A. Const.Amend. 1; West's V.C.A. § 59.1–443.2.

[9] Federal Courts 170B ⇐3616(1)

170B Federal Courts
170BXVII Courts of Appeals
170BXVII(K) Scope and Extent of Review
170BXVII(K)2 Standard of Review
170Bk3612 Remedial Matters
170Bk3616 Injunction
170Bk3616(1) k. In general. Most Cited Cases
(Formerly 170Bk862, 170Bk814.1, 170Bk776)

Court of Appeals reviews an order granting an injunction for an abuse of discretion, reviewing factual findings for clear error and legal conclusions de novo.

[10] Constitutional Law 92 ⇐2604

92 Constitutional Law
92XX Separation of Powers
92XX(C) Judicial Powers and Functions
92XX(C)6 Advisory Opinions
92k2603 Particular Issues and Applications
92k2604 k. In general. Most Cited Cases
(Formerly 170Bk2137, 170Bk13)

Court lacked jurisdiction, on motion to impose permanent injunction to bar enforcement of Virginia statute against privacy advocate, to decide question of whether First Amendment prohibited enfor-

cing statute, which barred intentional communication of another individual's Social Security number (SSN), against advocate for publishing on her website public records containing unredacted SSNs and that she allegedly obtained from other states' websites as any determination would have been analogous to rendering advisory opinion; record did not indicate from which states advocate obtained such records, whether those records had previously been publicly disclosed, or how those states protected SSNs from public disclosure, advocate failed to develop any legal theory explaining why court's First Amendment analysis about Virginia records also encompassed public records from other states, and Virginia's attorney general did not believe that statute reached non-Virginia public records and seemed opposed to prosecuting advocate for publishing such records. U.S.C.A. Const.Amend. 1; West's V.C.A. § 59.1–443.2.

[11] Federal Courts 170B ⚖2103

170B Federal Courts
170BIII Case or Controversy Requirement
170BIII(A) In General
170Bk2103 k. Nature of dispute; concreteness. Most Cited Cases
(Formerly 170Bk12.1)

Federal courts' judicial power may be exercised only where conflicting contentions of the parties present a real, substantial controversy between parties having adverse legal interests, a dispute definite and concrete, not hypothetical or abstract. U.S.C.A. Const. Art. 3, § 2, cl. 1.

[12] Federal Courts 170B ⚖2121

170B Federal Courts
170BIII Case or Controversy Requirement
170BIII(A) In General
170Bk2118 Ripeness; Prematurity
170Bk2121 k. Nature of dispute; concreteness. Most Cited Cases
(Formerly 170Bk12.1)

"Doctrine of ripeness" prevents the courts, through avoidance of premature adjudication, from entangling themselves in abstract disagreements.

[13] Federal Courts 170B ⚖2120

170B Federal Courts
170BIII Case or Controversy Requirement
170BIII(A) In General
170Bk2118 Ripeness; Prematurity
170Bk2120 k. Fitness and hardship. Most Cited Cases
(Formerly 170Bk12.1)

Federal courts assess ripeness by balancing the fitness of the issues for judicial decision with the hardship to the parties of withholding court consideration.

[14] Civil Rights 78 ⚖1456

78 Civil Rights
78III Federal Remedies in General
78k1449 Injunction
78k1456 k. Other particular cases and contexts. Most Cited Cases

Records 326 ⚖31

326 Records
326II Public Access
326II(A) In General
326k31 k. Regulations limiting access; offenses. Most Cited Cases

Permanent injunction, which barred Virginia from punishing privacy advocate for republishing on her website public land records that contained unredacted Social Security numbers (SSNs) of various state legislators, executive officers, and clerks of court as part of advocate's effort to reform Virginia's practice of publishing SSNs online, was not properly tailored to fit nature and extent of state's First Amendment violation; injunction did not protect advocate in republishing private individuals' SSNs or from republishing land records involving non-Virginia public officials, and there was no basis for treating those records differently from those involving Virginia public officials. U.S.C.A. Const.Amend. 1; West's V.C.A. § 59.1–443.2.

[15] Civil Rights 78 ⚖1450

78 Civil Rights
78III Federal Remedies in General
78k1449 Injunction
78k1450 k. In general. Most Cited Cases

Injunction 212 ⚖1015

212 Injunction
212I Injunctions in General; Permanent Injunctions in General
212I(A) Nature, Form, and Scope of Remedy
212k1013 Scope of Relief in General
212k1015 k. Discretion as to scope of relief. Most Cited Cases
(Formerly 212k189)

District courts have broad discretion when fashioning injunctive relief, but their powers are not boundless; once a constitutional violation is found, the court is required to tailor the scope of the remedy to fit the nature and extent of the constitutional violation.

*265 **ARGUED:** Earle Duncan Getchell, Jr., Office of the Attorney General of Virginia, Richmond, Virginia, for Appellant/Cross-Appellee. Rebecca Kim Glenberg, American Civil Liberties Union Foundation of Virginia, Richmond, Virginia, for Appellee/Cross-Appellant. **ON BRIEF:** William C. Mims, Attorney General of Virginia, Stephen R. McCullough, State Solicitor General, William E. Thro, Special Counsel, Martin L. Kent, Chief Deputy Attorney General, Stephen M. Hall, Assistant Attorney General, Office of the Attorney General of Virginia, Richmond, Virginia, for Appellant/Cross-Appellee. Frank M. Feibelman, Cooperating Attorney, ACLU of Virginia, Richmond, Virginia, for Appellee/Cross-Appellant. Marc Rotenberg, John Verdi, Jared Kaprove, Matthew Phillips, Electronic Privacy Information Center, Washington, D.C., for Amicus Supporting Appellee/Cross-Appellant.

Before DUNCAN and DAVIS, Circuit Judges, and Joseph R. GOODWIN, Chief United States District Judge for the Southern District of West Virginia, sitting by designation.

*266 Affirmed in part, reversed in part, and remanded by published opinion. Judge DUNCAN wrote the opinion, in which Judge DAVIS and Judge GOODWIN concurred. Judge DAVIS wrote a separate concurring opinion.

OPINION

DUNCAN, Circuit Judge:

This appeal arises from a First Amendment challenge to Virginia's Personal Information Privacy Act, Va.Code §§ 59.1–442 to –444. Section 59.1–443.2 prohibits "[i]ntentionally communicat[ing] another individual's social security number to the general public." The district court found this section unconstitutional as applied to an advocacy website that criticized Virginia's release of private information and showed publicly available Virginia land records containing unredacted Social Security numbers ("SSNs"). *Ostergren v. McDonnell*, No. 08–362, 2008 WL 3895593, at *14 (E.D.Va. Aug. 22, 2008). Later, the court entered a permanent injunction barring Virginia from punishing the republication of "publicly obtainable documents containing unredacted SSNs of Virginia legislators, Virginia Executive Officers or Clerks of Court as part as [sic] an effort to reform Virginia law and practice respecting the publication of SSNs online." *Ostergren v. McDonnell*, 643 F.Supp.2d 758, 770 (E.D.Va.2009). Both decisions are challenged on appeal. For the reasons that follow, we affirm in part and reverse in part.

I.

Betty Ostergren resides in Hanover County, Virginia, and advocates for information privacy across the country. Calling attention to Virginia's practice of placing land records on the Internet without first redacting SSNs, she displayed copies of Virginia land records containing unredacted SSNs on her website. After section 59.1–443.2 was

amended to prohibit this practice, but before the amendment took effect in July 2008, Ostergren brought this constitutional challenge.[FN1]

FN1. We provide factual background primarily through July 2008. Regarding the district court's decision finding section 59.1–443.2 unconstitutional, we cannot consider later factual developments because the record below did not extend beyond July 2008. *See Kirkpatrick v. Lenoir County Bd. of Educ.*, 216 F.3d 380, 384 (4th Cir.2000) ("From a procedural standpoint, courts hearing a case on appeal are limited to reviewing the record that has been developed below."). Regarding injunctive relief, we could theoretically have considered factual background through June 2009, but the record below contains little evidence about factual developments after July 2008.

A.

The clerk of court for each county in Virginia maintains documents affecting real property within the county. These "land records" reflect the ownership, conveyance, encumbrance, or financing of real property.[FN2] They include deeds, contracts, liens, divorce decrees, and various other documents. *See* Va.Code § 17.1–227. Virginia law requires that clerks make land records available for public inspection. *See* Va.Code § 17.1–208. Any person can review and copy land records by visiting the courthouse and requesting them.

FN2. Virginia law states that " '[l]and records' means any writing authorized by law to be recorded on paper or in electronic format that the clerk records affecting title to real property...." Va.Code § 17.1–292(B).

During the 1990s, many clerks of court began placing land records on the Internet. According to counsel for the Attorney General, the impetus came mainly *267 from the real estate industry because online access to land records facilitated numerous real estate transactions. The Virginia General Assembly encouraged this practice by allowing clerks to charge a fee for online access. *See* Va.Code § 17.1–276. The General Assembly later established a "Technology Trust Fund Fee" assessed for every document recorded, and set aside the revenue for improving access to public records through information technology. *See* Va.Code § 17.1–279. The General Assembly also declared "the intent ... that all circuit court clerks provide secure remote access to land records on or before July 1, 2006." 2004 Va. Acts 980. Finally, in 2007, the General Assembly imposed guidelines for posting land records online, *see* Va.Code § 17.1–294, and required that "[e]very circuit court clerk shall provide secure remote access to land records ... on or before July 1, 2008," Va.Code § 17.1–279(D)(3).

The parties stipulated that "[u]nder Virginia's 'secure remote access' system, any person may, for a nominal fee, obtain online access to all of the land records for a given locality." J.A. 86. Guidelines require that an individual must register and obtain a username and password before using the system. *See* Information Technology Resource Management Standard, SEC503–02 §§ 1.4(3), 2.1 (Va. Info. Techs. Agency Mar. 28, 2005). This involves signing an agreement, paying a fee (possibly several hundred dollars per year), and providing certain personal information (first and last names, business name, mailing address, telephone number, email address, and citizenship status). *Id.* § 2.1.1. "Registration must be in person or by means of a notarized or otherwise sworn application that establishes the prospective Subscriber's identity, business or residence address, and citizenship status." *Id.* § 2.1.2.

By July 2008, every county in Virginia had made its land records available on the Internet through secure remote access. This included over 200 million Virginia land records.

B.

Virginia's decision to place land records online

raised certain concerns about information privacy. For many decades, attorneys included SSNs on real estate documents submitted for recording. Initially assigned for the purpose of administering Social Security laws, nine-digit SSNs have become widely used for identification and account authentication by government agencies and private organizations because no two people have the same number. They are thus highly susceptible to misuse. An unscrupulous individual who knows another's SSN could, for example, obtain fraudulent credit cards or order new checks on that person's account.

When clerks of court began placing land records online, they did nothing to redact SSNs. At that time, Virginia law neither required such redaction nor prevented attorneys from submitting documents for recording that contained unredacted SSNs. In 2003 and 2004, however, the General Assembly provided that "clerk[s] may refuse to accept any instrument submitted for recordation that includes a grantor's, grantee's or trustee's social security number," and clarified that "the attorney or party who prepares or submits the instrument has responsibility for ensuring that the social security number is removed from the instrument prior to the instrument being submitted for recordation." Va.Code § 17.1–227. Virginia law also provides that clerks "shall be immune from suit arising from any acts or omissions relating to providing secure remote access to land records pursuant to this section unless the clerk was grossly negligent or *268 engaged in willful misconduct." Va.Code § 17.1–294(D).

The General Assembly finally addressed redaction in the 2007 legislation mandating that clerks provide secure remote access by July 1, 2008. *See* Va.Code § 17.1–279(D)(3). The General Assembly noted clerks' authority to redact SSNs from digital land records available through secure remote access, authorized hiring private vendors to run redaction software, and authorized using Technology Trust Fund money for this purpose. *See* Va.Code § 17.1–279. The legislation would have also required clerks to complete the redaction process by July 1, 2010, but this provision never went into effect because the General Assembly failed to appropriate the necessary funds. *See* 2007 Va. Acts 872; 2007 Va. Acts 748. These efforts focused solely on digital land records available online. Virginia does not redact SSNs from original land records maintained at local courthouses even though Virginia law requires that such records remain publicly accessible.

The redaction process involves two steps—one electronic, the other manual. First, computer software checks digital land records and, in essence, labels each document "SSN found," "SSN probably found," "SSN possibly found," and "SSN not found." Individuals then manually review all but the last category, which they randomly sample. According to stipulation,

> The accuracy of the redaction methods used by the circuit court clerks with regard to images that actually have social security numbers is between 95% and 99%. After redaction, a social security number that remains un-redacted in the online land records will be redacted if the Clerk is informed of the inaccuracy. If not brought to the Clerk's attention, it will remain accessible in the online land records.

J.A. 230. One company, Computing System Innovations ("CSI"), handled redaction for 67 counties. In processing about 50 million images, CSI manually reviewed about 5 million and discovered that 1,575,422 (about 3.21%) contained SSNs.[FN3]

> FN3. Ostergren testified that on July 15, 2008, after Hanover County purportedly finished redacting SSNs, she successfully located Hanover County land records containing unredacted SSNs through secure remote access.

By July 2008, 105 of Virginia's 120 counties reported that they had completed the redaction process. Among the 15 that remained, two planned to

finish by July 2010 and the rest planned to finish by December 2009. Despite the incomplete redaction, these 15 counties nonetheless continued to make their land records available online through secure remote access.

C.

When Virginia clerks of court started placing land records containing unredacted SSNs online, Ostergren began lobbying the General Assembly in opposition and contacting individuals whose SSNs were compromised. She has engaged in similar advocacy across the country, but such advocacy alone met with little success. Ostergren created her website www. The Virginia Watchdog. com in 2003 and, two years later, began posting copies of public records containing unredacted SSNs obtained from government websites. Since then, Ostergren has posted numerous Virginia land records showing SSNs that she herself obtained through Virginia's secure remote access website. For example, she explained that searching for the term "Internal Revenue Service," "Department of Justice," or "United States" produces *269 thousands of federal tax liens, and all those filed before 2006 contain SSNs.

In posting records online, Ostergren seeks to publicize her message that governments are mishandling SSNs and generate pressure for reform. FN4 She explained that "seeing a document containing an SSN posted on my website makes a viewer understand instantly, at a gut level, why it is so important to prevent the government from making this information available on line [sic]." J.A. 89. She added that merely explaining the problem lacks even "one-tenth the emotional impact that is conveyed by the document itself, posted on the website." J.A. 89. Perhaps for this reason, Ostergren received considerable media attention when she began posting records online. Furthermore, many government agencies outside Virginia responded by removing public records from the Internet or redacting private information.

FN4. Normally Ostergren reveals only public officials' SSNs, reasoning that they are "the people who have the influence to address the problem." J.A. 89. She explained, however, that in June 2008 the clerk of court for Pulaski County, Arkansas, refused to remove land records from the Internet pending SSN redaction until Ostergren published land records that showed several prominent local citizens' SSNs.

Despite this success, Ostergren's website has also contributed to the underlying social concern that motivates her advocacy. Because one can visit her website and find public records showing SSNs without needing to register or input search terms, Ostergren makes Virginia land records showing SSNs more accessible to the public than they are through Virginia's secure remote access system. Potential wrongdoers not experienced or motivated enough to register for secure remote access might nonetheless stumble upon Ostergren's website and obtain SSNs. Indeed, one person has pleaded guilty to using Ostergren's website to obtain fraudulent credit cards.

D.

The controversy that spurred this case arose from Ostergren's disclosure of others' SSNs printed in Virginia land records that she posted online. Section 59.1–443.2 of the Code of Virginia provides that "a person shall not ... [i]ntentionally communicate another individual's social security number to the general public." Va.Code § 59.1–443.2(A)(1). In Spring 2008, the General Assembly removed a statutory exception for "records required by law to be open to the public." FN5 2008 Va. Acts 837. The Attorney General of Virginia later indicated that, after this change took effect on July 1, 2008, Ostergren would be prosecuted under section 59.1–443.2 for publicly disseminating Virginia land records containing unredacted SSNs. FN6

FN5. Ostergren alleges that the General Assembly made this change "in direct response to [her] website." J.A. 10.

FN6. For a section 59.1–443.2 violation, the Attorney General may seek various civil penalties, including fines and injunctions. *See* Va.Code §§ 59.1–201 to –206. Furthermore, "[a]ny person who suffers loss as the result of a violation" may "initiate an action to recover actual damages, or $500, whichever is greater," or for a willful violation, "an amount not exceeding three times the actual damages sustained, or $1,000, whichever is greater," plus "reasonable attorneys' fees and court costs." Va.Code § 59.1–204.

On June 11, 2008, Ostergren brought this action in the Eastern District of Virginia under 42 U.S.C. § 1983 seeking declaratory and injunctive relief, and attorney's fees and costs. She contended that enforcing section 59.1–443.2 against her for publishing copies of public records lawfully obtained from a government website violates the First Amendment. During a ***270** hearing on Ostergren's motion for preliminary injunctive relief, Virginia's Attorney General agreed not to enforce the statute against Ostergren while this action remains pending.

On August 22, 2008, the district court concluded, based upon stipulated facts, that "Virginia Code § 59.1–443.2 is unconstitutional as applied to Ostegren's [sic] website as it presently exists." *Ostergren*, 2008 WL 3895593, at *14. On June 2, 2009, after further briefing and argument about injunctive relief, the court entered

> a permanent injunction ... against enforcement of Va.Code § 59.1–443.2 against any iteration of Ostergren's website, now or in the future, that simply republishes publicly obtainable documents containing unredacted SSNs of Virginia legislators, Virginia Executive Officers or Clerks of Court as part as [sic] an effort to reform Virginia law and practice respecting the publication of SSNs online.

Ostergren, 643 F.Supp.2d at 770. The Attorney General appealed, challenging the district court's August 22, 2008, constitutional determination. Ostergren cross-appealed, arguing that the June 2, 2009, award of injunctive relief was too narrow. We consider the appeal and cross-appeal below.

II.

First we review the district court's August 22, 2008, constitutional determination. "We review de novo a properly preserved constitutional claim." *United States v. Hall*, 551 F.3d 257, 266 (4th Cir.2009). Virginia argues that SSNs are categorically unprotected speech that may be prohibited entirely. Alternatively, Virginia argues that the state interest in preserving citizens' privacy by limiting SSNs' public disclosure justifies barring Ostergren's speech. In other words, Virginia maintains that the First Amendment does not apply here and that, even if it does, enforcing section 59.1–443.2 against Ostergren should survive First Amendment scrutiny. We address each argument in turn.[FN7]

FN7. Virginia challenged standing and ripeness before the district court but not on appeal. We observe that standing and ripeness are established merely to satisfy ourselves of our jurisdiction. Although no prosecution occurred, Ostergren has standing because the Attorney General planned to initiate prosecution and section 59.1–443.2 was recently amended to reach her speech. *See N.C. Right to Life, Inc. v. Bartlett*, 168 F.3d 705, 710 (4th Cir.1999) ("A non-moribund statute that facially restricts expressive activity by the class to which the plaintiff belongs presents ... a credible threat [of prosecution], and a case or controversy thus exists in the absence of compelling evidence to the contrary." (internal quotations and alterations omitted)); *Mobil Oil Corp. v. Att'y Gen. of Va.*, 940 F.2d 73, 76 (4th Cir.1991) (holding that where a law was recently amended to cover conduct at issue "[i]t would be unreasonable to assume" that the government

made that change "without intending that it be enforced"). Furthermore, Ostergren's constitutional claim regarding publishing Virginia land records appears ripe because "[t]he factual situation is well-developed," there are "no material facts that are in dispute," and "[t]he parties argue only on the application of the law." *Ostergren*, 2008 WL 3895593, at *5; *see Miller v. Brown*, 462 F.3d 312, 319 (4th Cir.2006) ("balanc[ing] the fitness of the issues for judicial decision with the hardship to the parties of withholding court consideration" to assess ripeness and noting that "[a] case is fit for judicial decision when the issues are purely legal and when the action in controversy is final and not dependent on future uncertainties" (internal quotations omitted)).

A.

[1] The First Amendment's protection of "freedom of speech, or of the press," was designed to allow individuals to criticize their government without fear. U.S. Const. amend. I; *see* *271*Gentile v. State Bar of Nev.*, 501 U.S. 1030, 1034, 111 S.Ct. 2720, 115 L.Ed.2d 888 (1991) ("There is no question that speech critical of the exercise of the State's power lies at the very center of the First Amendment."); *New York Times Co. v. Sullivan*, 376 U.S. 254, 273, 84 S.Ct. 710, 11 L.Ed.2d 686 (1964) (calling liberty to criticize government conduct "the central meaning of the First Amendment"). This protection also precludes the government from silencing the expression of unpopular ideas. *See Police Dep't of Chi. v. Mosley*, 408 U.S. 92, 95, 92 S.Ct. 2286, 33 L.Ed.2d 212 (1972) ("[T]he First Amendment means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content."). Accordingly, laws restricting the content of expression normally are invalid under the First Amendment unless narrowly tailored to promote a compelling state interest. *See United States v. Playboy Entm't Group, Inc.*, 529 U.S. 803, 813, 120 S.Ct. 1878, 146 L.Ed.2d 865 (2000) ("If a statute regulates speech based on its content, it must be narrowly tailored to promote a compelling Government interest."); *see also R.A. V. v. City of St. Paul*, 505 U.S. 377, 382, 112 S.Ct. 2538, 120 L.Ed.2d 305 (1992) ("Content-based regulations are presumptively invalid.").

[2] The Supreme Court has nevertheless identified certain categories of "unprotected" speech that may be circumscribed entirely. Fighting words, obscenity, incitement of illegal activity, and child pornography are examples. *See Chaplinsky v. New Hampshire*, 315 U.S. 568, 571–72, 62 S.Ct. 766, 86 L.Ed. 1031 (1942); *Roth v. United States*, 354 U.S. 476, 485, 77 S.Ct. 1304, 1 L.Ed.2d 1498 (1957); *Brandenburg v. Ohio*, 395 U.S. 444, 447–48, 89 S.Ct. 1827, 23 L.Ed.2d 430 (1969); *New York v. Ferber*, 458 U.S. 747, 764, 102 S.Ct. 3348, 73 L.Ed.2d 1113 (1982); *see also Schenck v. United States*, 249 U.S. 47, 52, 39 S.Ct. 247, 63 L.Ed. 470 (1919) ("The most stringent protection of free speech would not protect a man in falsely shouting fire in a theatre and causing a panic."). The Court has said that these categories of unprotected speech "are no essential part of any exposition of ideas, and are of such slight social value as a step to truth that any benefit that may be derived from them is clearly outweighed by the social interest in order and morality." *Chaplinsky*, 315 U.S. at 572, 62 S.Ct. 766.

[3] Virginia argues that the unredacted SSNs on Ostergren's website should not be protected under the First Amendment because they facilitate identity theft and are no essential part of any exposition of ideas. *See* Eugene Volokh, *Crime–Facilitating Speech*, 57 Stan. L.Rev. 1095, 1146–47 (2005) (arguing that SSNs and computer passwords are "categories of speech that are likely to have virtually no noncriminal uses" and that "[r]estricting the publication of full social security numbers or passwords ... will not materially interfere with valuable speech"). Although these observations might be true under certain circumstances,

we cannot agree with Virginia's argument here. The unredacted SSNs on Virginia land records that Ostergren has posted online are integral to her message. Indeed, they *are* her message. Displaying them proves Virginia's failure to safeguard private information and powerfully demonstrates why Virginia citizens should be concerned.[FN8] *Cf.* *272 *United States v. Hubbell*, 530 U.S. 27, 36–37, 120 S.Ct. 2037, 147 L.Ed.2d 24 (2000) (noting that "the act of producing documents in response to a subpoena ... may implicitly communicate statements of fact" because "[b]y producing documents ... the witness would admit that the papers existed, were in his possession or control, and were authentic" (internal quotations omitted)).

> FN8. Virginia argues that Ostergren could redact several digits from each SSN and still express her message. But the First Amendment protects Ostergren's freedom to decide how her message should be communicated. Although wearing a jacket bearing the words "Boo for the Draft" rather than "Fuck the Draft" may convey the same political critique, the Supreme Court found that the government cannot prohibit the more offensive version. *Cohen v. California*, 403 U.S. 15, 24, 91 S.Ct. 1780, 29 L.Ed.2d 284 (1971) (noting "the usual rule that governmental bodies may not prescribe the form or content of individual expression"). The Court explained:
>
> > [M]uch linguistic expression serves a dual communicative function: it conveys not only ideas capable of relatively precise, detached explication, but otherwise inexpressible emotions as well. In fact, words are often chosen as much for their emotive as their cognitive force. We cannot sanction the view that the Constitution, while solicitous of the cognitive content of individual speech has little or no regard for that emotive function which practically speaking, may often be the more important element of the overall message sought to be communicated.
>
> *Id.* at 26, 91 S.Ct. 1780. Furthermore, partial redaction would diminish the documents' shock value and make Ostergren less credible because people could not tell whether she or Virginia did the partial redaction. *See Ross v. Midwest Commc'ns, Inc.*, 870 F.2d 271, 274 (5th Cir.1989) (holding that disclosing a rape victim's name in a documentary about the convicted man's potential innocence was "of unique importance to the credibility and persuasive force of the story"); *Gilbert v. Med. Econ. Co.*, 665 F.2d 305, 308 (10th Cir.1981) (regarding an article about medical malpractice that disclosed a doctor's name and photograph, finding that "these truthful representations ... strengthen the impact and credibility of the article" because "[t]hey obviate any impression that the problems raised in the article are remote or hypothetical, thus providing an aura of immediacy and even urgency that might not exist had plaintiff's name and photograph been suppressed").

We find particularly significant just how Ostergren communicates SSNs. She does not simply list them beside people's names but rather provides copies of entire documents maintained by government officials. Given her criticism about how public records are managed, we cannot see how drawing attention to the problem by displaying those very documents could be considered unprotected speech. Indeed, the Supreme Court has deemed such speech particularly valuable within our society:

> Public records by their very nature are of interest to those concerned with the administration of government, and a public benefit is performed by the reporting of the true contents of the records by the media. The freedom of the press to publish

that information appears to us to be of critical importance to our type of government in which the citizenry is the final judge of the proper conduct of public business.

Cox Broad. Corp. v. Cohn, 420 U.S. 469, 495, 95 S.Ct. 1029, 43 L.Ed.2d 328 (1975). Thus, although we do not foreclose the possibility that communicating SSNs might be found unprotected in other situations, we conclude, on these facts, that the First Amendment does reach Ostergren's publication of Virginia land records containing unredacted SSNs.[FN9]

FN9. After this appeal was briefed and orally argued, the Supreme Court clarified that *Chaplinsky* does not provide a sufficient test for identifying categories of unprotected speech because such categories derive from history and tradition. *See United States v. Stevens*, 559U.S. 460, 130 S.Ct. 1577, 1586, 176 L.Ed.2d 435 (2010) (declining to recognize a new category of unprotected speech for depictions of animal cruelty). The Court also disavowed "a freewheeling authority to declare new categories of speech outside the scope of the First Amendment," admitting only that "[m]aybe there are some categories of speech that have been historically unprotected, but have not yet been specifically identified or discussed as such in our case law." *Id.* Because we already find Virginia's argument unpersuasive, we need not also conduct the historical analysis that *Stevens* would require.

*273 B.

[4] We next consider whether enforcing section 59.1–443.2 against Ostergren for posting online Virginia land records containing unredacted SSNs survives First Amendment scrutiny. Although Ostergren's political speech criticizing Virginia "lies at the very center of the First Amendment," *Gentile*, 501 U.S. at 1034, 111 S.Ct. 2720, publishing SSNs online undermines individual privacy. Freedom of speech must therefore be weighed against the "right of privacy" which the Supreme Court has also recognized. *See Cox Broad.*, 420 U.S. at 488, 95 S.Ct. 1029 (recognizing "the so-called right of privacy"). The Court tried to strike that balance in *Cox Broadcasting* and subsequent cases involving restrictions on truthful publication of private information. Because we must decide where this case fits within that balance, we begin our analysis by reviewing those decisions.

In *Cox Broadcasting*, the Supreme Court ruled that the First Amendment prohibits a lawsuit against a television station for broadcasting a rape victim's name when the station learned her identity from a publicly available court record. The issue arose in the context of six youths being indicted for rape and murder. Although their case garnered substantial press attention, the victim's identity was not disclosed because Georgia law prohibited "publish[ing] or broadcast[ing] the name or identity of a rape victim." *Id.* at 472, 95 S.Ct. 1029. During trial, the clerk of court showed a reporter the indictments even though they clearly stated the victim's full name. The reporter later explained, "[N]o attempt was made by the clerk or anyone else to withhold the name and identity of the victim from me or from anyone else and the said indictments apparently were available for public inspection upon request." *Id.* at 472 n. 3, 95 S.Ct. 1029. When the television station employing the reporter later broadcast the victim's name, her father sued for money damages. The Georgia Supreme Court held that his "complaint stated a cause of action 'for the invasion of the ... right of privacy, or for the tort of public disclosure,' " and rejected the station's First Amendment defense. *Id.* at 474, 95 S.Ct. 1029 (quoting *Cox Broad. Corp. v. Cohn*, 231 Ga. 60, 200 S.E.2d 127, 130 (1973)).

The Supreme Court reversed. Although recognizing "a strong tide running in favor of the so-called right of privacy," *id.* at 488, 95 S.Ct. 1029, the Court reasoned that "the interests in privacy fade when the information involved already appears

on the public record," *id.* at 494–95, 95 S.Ct. 1029. The Court observed that "[b]y placing the information in the public domain on official court records, the State must be presumed to have concluded that the public interest was thereby being served." *Id.* at 495, 95 S.Ct. 1029. The Court also discussed the importance of truthful reporting about public records and expressed reluctance to create a doctrine that "would invite timidity and self-censorship and very likely lead to the suppression of many items that ... should be made available to the public." *Id.* at 496, 95 S.Ct. 1029. The Court concluded:

> At the very least, the First and Fourteenth Amendments will not allow exposing the press to liability for truthfully publishing information released to the public in official court records.... Once true information is disclosed in public court documents open to public inspection, the press cannot be sanctioned for publishing it.

*274 *Id.* The Court explained that "[i]f there are privacy interests to be protected in judicial proceedings, the States must respond by means which avoid public documentation or other exposure of private information." *Id.*

Although *Cox Broadcasting* avoided deciding whether truthful publication may ever be punished, subsequent cases helped to clarify the relevant inquiry. In *Oklahoma Publishing Co. v. District Court*, 430 U.S. 308, 97 S.Ct. 1045, 51 L.Ed.2d 355 (1977), the Supreme Court held that a trial court could not bar newspapers from publishing a juvenile offender's name learned during a court proceeding open to the public. The Court explained, " 'Once a public hearing ha[s] been held, what transpired there [can]not be subject to prior restraint.' " *Id.* at 311, 97 S.Ct. 1045 (quoting *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 568, 96 S.Ct. 2791, 49 L.Ed.2d 683 (1976)). In *Landmark Communications, Inc. v. Virginia*, 435 U.S. 829, 98 S.Ct. 1535, 56 L.Ed.2d 1 (1978), the Court held that Virginia could not punish a newspaper for publishing correct information that had been leaked about confidential proceedings by the Virginia Judicial Inquiry and Review Commission. The Court reasoned that Virginia's interests in preserving respect for courts and protecting individual judges' reputations did not justify prohibiting speech that "clearly served those interests in public scrutiny and discussion of governmental affairs which the First Amendment was adopted to protect." *Id.* at 839, 98 S.Ct. 1535.

The Supreme Court later articulated a constitutional standard based upon these decisions. In *Smith v. Daily Mail Publishing Co.*, 443 U.S. 97, 99 S.Ct. 2667, 61 L.Ed.2d 399 (1979), the Court observed that *Cox Broadcasting*, *Oklahoma Publishing*, and *Landmark Communications* "all suggest strongly that if a newspaper lawfully obtains truthful information about a matter of public significance then state officials may not constitutionally punish publication of the information, absent a need to further a state interest of the highest order." *Daily Mail*, 443 U.S. at 103, 99 S.Ct. 2667. This case involved two newspapers convicted under a West Virginia statute that barred publishing the names of juvenile offenders without court approval. Reporters had learned certain juvenile offenders' names by questioning witnesses, police officers, and the prosecutor. The Supreme Court invalidated the convictions because West Virginia's interest in protecting juvenile offenders' anonymity was insufficiently important and "there [was] no evidence to demonstrate that the imposition of criminal penalties [was] necessary to protect the confidentiality of juvenile proceedings." *Id.* at 105, 99 S.Ct. 2667.

After this flurry of decisions, the Supreme Court applied the *Daily Mail* standard roughly a decade later in another case about a rape victim. In *The Florida Star v. B.J.F.*, 491 U.S. 524, 109 S.Ct. 2603, 105 L.Ed.2d 443 (1989), the appellee B.J.F. reported to local police that she had been robbed and sexually assaulted. Despite its internal policy against revealing names of rape victims, the police department inadvertently placed a police report containing B.J.F.'s name in its press room. The department did not restrict access to the press room or to reports made available therein. After a reporter

copied the police report verbatim, an area newspaper published an article containing B.J.F.'s full name. She sued for money damages, claiming the newspaper had been per se negligent because Florida law prohibited printing, publishing, or broadcasting names of rape victims in any instrument of mass communication. During trial, B.J.F. testified that publicity of her rape made her suffer extreme embarrassment, receive*275 additional threats of rape, change her phone number and residence, seek police protection, and obtain medical health counseling. The jury awarded damages and a Florida appellate court affirmed, rejecting the newspaper's First Amendment defense.

The Supreme Court reversed. Before applying the *Daily Mail* standard regarding truthful publication of lawfully obtained information, the Court noted three underlying considerations that justified this analytical approach. First, that the standard covers only lawfully obtained information means that the government retains ample means of protecting interests that might be threatened by publication. This consideration has additional implications when the government itself initially holds the information:

> To the extent sensitive information is in the government's custody, it has even greater power to forestall or mitigate the injury caused by its release. The government may classify certain information, establish and enforce procedures ensuring its redacted release, and extend a damages remedy against the government or its officials where the government's mishandling of sensitive information leads to its dissemination. Where information is entrusted to the government, a less drastic means than punishing truthful publication almost always exists for guarding against the dissemination of private facts.

Id. at 534, 109 S.Ct. 2603. Second, "punishing the press for its dissemination of information which is already publicly available is relatively unlikely to advance the interests in the service of which the State seeks to act." *Id.* at 535, 109 S.Ct. 2603. The Court added that "where the government has made certain information publicly available, it is highly anomalous to sanction persons other than the source of its release." *Id.* Third, " 'timidity and self-censorship' ... may result from allowing the media to be punished for publishing certain truthful information." *Id.* (quoting *Cox Broad.*, 420 U.S. at 496, 95 S.Ct. 1029). The Court explained that, where the government discloses private information, not protecting its publication "would force upon the media the onerous obligation of sifting through government press releases, reports, and pronouncements to prune out material arguably unlawful for publication ... even where the newspaper's sole object was to reproduce, with no substantial change, the government's rendition of the event in question." *Id.* at 536, 109 S.Ct. 2603. Having reiterated these considerations, the Court endorsed the *Daily Mail* standard: "We hold ... that where a newspaper publishes truthful information which it has lawfully obtained, punishment may lawfully be imposed, if at all, only when narrowly tailored to a state interest of the highest order." *Id.* at 541, 109 S.Ct. 2603.

Applying this standard, the Supreme Court found that the newspaper article about B.J.F. truthfully published lawfully obtained information about a matter of public significance. The Court also found that punishing the newspaper was not narrowly tailored to Florida's interest in preserving rape victims' privacy because the police department itself could have initially withheld the sensitive information.[FN10] That *276 the department's disclosure was actually inadvertent was immaterial. *See id.* at 538, 109 S.Ct. 2603 ("B.J.F.'s identity would never have come to light were it not for the erroneous, if inadvertent, inclusion by the Department of her full name in an incident report made available in a pressroom open to the public."). The Court concluded: "Where, as here, the government has failed to police itself in disseminating information, it is clear under *Cox Broadcasting*, *Oklahoma Publishing*, and *Landmark Communications* that the imposition of damages against the press for its sub-

sequent publication can hardly be said to be a narrowly tailored means of safeguarding anonymity." *Id.*

> FN10. Notably, the Court expressly avoided deciding whether Florida's asserted interest constituted "a state interest of the highest order"—resolving the case instead solely on narrow-tailoring grounds. *Daily Mail*, 443 U.S. at 103, 99 S.Ct. 2667; *see Florida Star*, 491 U.S. at 537, 109 S.Ct. 2603 ("At a time in which we are daily reminded of the tragic reality of rape, it is undeniable that these are highly significant interests, a fact underscored by the Florida Legislature's explicit attempt to protect these interests by enacting a criminal statute prohibiting much dissemination of victim identities. We accordingly do not rule out the possibility that, in a proper case, imposing civil sanctions for publication of the name of a rape victim might be so overwhelmingly necessary to advance these interests as to satisfy the *Daily Mail* standard.").

Notably, *Cox Broadcasting* and its progeny avoided deciding the ultimate question of whether truthful publication could ever be prohibited. Each decision resolved this ongoing conflict between privacy and the First Amendment "only as it arose in a discrete factual context." *Florida Star*, 491 U.S. at 530, 109 S.Ct. 2603. The *Florida Star* Court noted that "the future may bring scenarios which prudence counsels our not resolving anticipatorily." *Id.* at 532, 109 S.Ct. 2603 (citing *Near v. Minnesota ex rel. Olson*, 283 U.S. 697, 716, 51 S.Ct. 625, 75 L.Ed. 1357 (1931) (hypothesizing "publication of the sailing dates of transports or the number and location of troops")).

Those decisions nonetheless make clear that Ostergren's constitutional challenge must be evaluated using the *Daily Mail* standard.[FN11] Accordingly, Virginia may enforce section 59.1–443.2 against Ostergren for publishing lawfully obtained, truthful information about a matter of public significance "only when narrowly tailored to a state interest of the highest order." *Id.* at 541, 109 S.Ct. 2603. Virginia concedes that Ostergren lawfully obtained and truthfully published the Virginia land records that she posted online. Moreover, this information plainly concerns "a matter of public significance," *Daily Mail*, 443 U.S. at 103, 99 S.Ct. 2667, because displaying the contents of public records and criticizing Virginia's release of private information convey political messages that concern the public, *see Cox Broad.*, 420 U.S. at 495, 95 S.Ct. 1029 ("Public records by their very nature are of interest to those concerned with the administration of government, and a public benefit is performed by the reporting of the true contents of the records by the media."); *Landmark Commc'ns*, 435 U.S. at 839, 98 S.Ct. 1535 (deeming the operation of government affairs "a matter of public interest"). Therefore, the only remaining issues are (1) whether Virginia has asserted a state interest of the highest order and (2) whether enforcing section 59.1–443.2 against Ostergren would be narrowly tailored to that interest. We address each in turn.

> FN11. Counsel for the Attorney General conceded during oral argument that, under this standard, Ostergren's advocacy website cannot be distinguished from a television station or newspaper. *See Sheehan v. Gregoire*, 272 F.Supp.2d 1135, 1145 (W.D.Wash.2003) (considering a website about police accountability "analytically indistinguishable from a newspaper" where the website "communicates truthful lawfully-obtained, publicly-available personal identifying information with respect to a matter of public significance").

1.

Virginia asserts that its interest in protecting individual privacy by limiting SSNs' public disclosure constitutes "a state *277 interest of the highest order." *Daily Mail*, 443 U.S. at 103, 99 S.Ct. 2667. Although noting that "it should not be difficult for a

court to conclude that the protection of SSNs from public disclosure should qualify as a State interest of the highest order," the district court reached the opposite conclusion upon reasoning that Virginia's conduct had been inconsistent with that interest. *Ostergren*, 2008 WL 3895593, at *10; *see id.* ("[T]he State's own conduct in making those SSNs publicly available through unredacted release on the Internet significantly undercuts the assertion ... that the State actually regards protection of SSNs as an interest of the highest order."). Before discussing this issue, we address the proper analytical framework for determining what constitutes a state interest of the highest order.

a.

In assessing Virginia's asserted interest, the district court put to one side that interest's actual importance and instead considered only whether Virginia itself considered the interest important—applying a subjective rather than objective standard. The court explained, "[I]t is not the perception of a federal court that defines a State interest of the highest order. Instead, it is the State's view and its conduct that, under accepted First Amendment jurisprudence, must supply the basis for such a conclusion." *Id.*; *see Ostergren*, 643 F.Supp.2d at 766 ("Whether the State has an interest of the highest order is answered by examining objectively the means by which the State treats the information in question."). The court later added, "When, as here, a State legislature has expressed its own view of the priority of a State interest, a federal court is not permitted to revise that view to save the statute." *Ostergren*, 2008 WL 3895593, at *11.

[5] In reaching this conclusion, the district court may have limited its consideration unnecessarily. In deciding what constitutes a state interest of the highest order, courts cannot be bound by "the State's view and its conduct." *Id.* at *10. For example, although a state government might demonstrate a fervent, consistently applied policy of punishing people for not cleaning up after their dogs, we would not therefore be compelled to consider this a state interest of the highest order. Conversely, although a state government might practice racial discrimination for decades—and many have—we would not therefore be barred from considering racial equality a state interest of the highest order. *See Regents of Univ. of Ca. v. Bakke*, 438 U.S. 265, 396, 98 S.Ct. 2733, 57 L.Ed.2d 750 (1978) (Marshall, J., concurring) ("In light of the sorry history of discrimination and its devastating impact on the lives of Negroes, bringing the Negro into the mainstream of American life should be a state interest of the highest order.").

[6] Furthermore, Supreme Court precedent applying the *Daily Mail* standard makes clear that objective criteria can be considered when deciding what constitutes a state interest of the highest order. In *Butterworth v. Smith*, 494 U.S. 624, 110 S.Ct. 1376, 108 L.Ed.2d 572 (1990), Florida maintained that its interest in preserving grand jury secrecy justified preventing a reporter from publicizing his own grand jury testimony. Concluding that Florida's asserted interest did not constitute a state interest of the highest order, the Court observed that the Federal Rules of Criminal Procedure contained no such requirement and that "only 14 States have joined Florida in imposing an obligation of secrecy on grand jury witnesses." *Id.* at 635, 110 S.Ct. 1376. The Court explained that, "[w]hile these practices are not conclusive *278 as to the constitutionality of Florida's rule, they are *probative of the weight to be assigned Florida's asserted interests* and the extent to which the prohibition in question is necessary to further them." *Id.* (emphasis added). FN12

FN12. We note that, contrary to the concurrence's suggestion, our First Amendment analysis does indeed involve "a fact-intensive inquiry into the state's view and its actual conduct in furthering its asserted interest." *Infra* at 291. We simply conduct that inquiry mainly regarding narrow-tailoring—the approach *Florida Star* em-

ployed—rather than regarding the state interest itself—the concurrence's preferred approach.

Despite concluding that a subjective standard was required, the district court nevertheless observed that "in concept, Va.Code § 59.1–443.2 furthers what ought to be, by any objective measure, a State interest of the highest order." *Ostergren*, 643 F.Supp.2d at 769. We turn now to that issue.

b.

We find it helpful to place our inquiry in historical context by discussing the genesis of modern privacy concerns surrounding SSNs. The Social Security Administration created SSNs in 1936 merely to track individuals' earnings and eligibility for Social Security benefits. They soon became used for other purposes, however, because SSNs provide unique permanent identification for almost every person. Indeed, the federal government was among the first to avail itself of their utility. In 1943, President Roosevelt ordered that any federal agency which "establish[es] a new system of permanent account numbers pertaining to individual persons" must "utilize exclusively the Social Security Act account numbers." Exec. Order No. 9397, 8 Fed.Reg. 16,095 (Nov. 30, 1943). Countless state and federal agencies later adopted the SSN, particularly during the 1960s. For example, Congress authorized the Internal Revenue Service to begin using the SSN for taxpayer identification in 1961. *See* Act of Oct. 5, 1961, Pub.L. No. 87–397, 75 Stat. 828 (1961). Private organizations, especially financial institutions, also started using the SSN for account identification and other purposes. Indeed, the Bank Records and Foreign Transactions Act, Pub.L. No. 91–508, 84 Stat. 1114 (1970), required banks, savings and loan associations, credit unions, and securities brokers and dealers to collect customers' SSNs. *See, e.g., id.* § 101 (requiring "the maintenance of appropriate types of records by insured banks of the United States where such records have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings").

Public concern about information privacy, however, soon increased. In 1973, the Department of Health, Education, and Welfare published an influential report warning about "an increasing tendency for the Social Security number to be used as if it were an SUI [standard universal identifier]." U.S. Department of Health, Education, and Welfare, Report of the Secretary's Advisory Committee on Automated Personal Data Systems: Records, Computers, and the Rights of Citizens xxxii (1973). Congress responded by enacting the Privacy Act of 1974, 5 U.S.C. § 552a, which prohibits government agencies from denying rights, privileges, or benefits because a person withholds his SSN. By enacting this statute, "Congress sought to curtail the expanding use of social security numbers by federal and local agencies and, by so doing, to eliminate the threat to individual privacy and confidentiality of information posed by common numerical identifiers." *Doyle v. Wilson*, 529 F.Supp. 1343, 1348 (D.Del.1982). The related Senate Report stated that widespread usage of SSNs was "one of the most serious manifestations*279 of privacy concerns in the Nation." S.Rep. No. 93–1183 (1974), *as reprinted in* 1974 U.S.C.C.A.N. 6916, 6943.

Since then, usage of SSNs by federal and local agencies, financial institutions, and other organizations has become nearly ubiquitous. Beyond simply matching records with accounts, these organizations also frequently use SSNs for account authentication. This means that the SSN provides a password that lets one modify account information. By consequence, the SSN has become a crucial piece of information allowing the creation or modification of myriad personal accounts. *See* U.S. Government Accountability Office, GAO No. 09–759T, Identity Theft: Governments Have Acted to Protect Personally Identifiable Information, but Vulnerabilities Remain 8 (calling the SSN "a vital piece of information needed to function in American society" and noting that "U.S. citizens generally need an SSN to pay taxes, obtain a driver's license, or open a bank account, among other things"). Unfortunately, for that reason, SSNs can easily be used to

commit identity theft—that is, tendering another's identifying information to carry out financial fraud or other criminal activity. *See* Jonathan J. Darrow & Stephen D. Lichtenstein, "*Do You Really Need My Social Security Number?" Data Collection Practices in the Digital Age*, 10 N.C. J.L. & Tech. 1, 4–5 (2008) ("Reflecting the unfortunate reality that a single number can provide access to multiple accounts, commentators have lamented that the social security number has become a 'skeleton key' for identity theft criminals."). One therefore has a considerable privacy interest in keeping his SSN confidential.

We previously considered this privacy interest in *Greidinger v. Davis*, 988 F.2d 1344 (4th Cir.1993). Invalidating a statute that required people to provide their SSN before they could vote and then publicly disclosed that confidential information, we observed:

> Since the passage of the Privacy Act, an individual's concern over his SSN's confidentiality and misuse has become significantly more compelling. For example, armed with one's SSN, an unscrupulous individual could obtain a person's welfare benefits or Social Security benefits, order new checks at a new address on that person's checking account, obtain credit cards, or even obtain the person's paycheck.

Id. at 1353; *see also City of Kirkland v. Sheehan*, No. 01–2–09513–7, 2001 WL 1751590, at *6 (Wash.Sup.Ct. May 10, 2001) ("[A]ccess to an SSN allows a person, agency or company to more efficiently and effectively search for and seize information and assets of another, a power originally available only to the government and one which was subject to direct Constitutional restraint."). We added that "the harm that can be inflicted from the disclosure of a SSN to an unscrupulous individual is alarming and potentially financially ruinous." *Greidinger*, 988 F.2d at 1354. On average, victims of identity theft lose about $17,000 and must spend over $1,000 and 600 hours of personal time cleaning up their credit reports. *See* Danielle Keats Citron, *Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age*, 80 S. Cal. L.Rev. 241, 253 (2007).

Reflecting these concerns, Congress and all 50 States have passed laws regulating SSN collection and disclosure. *See* Andrew Serwin, Information Security and Privacy §§ 22–23 (2009); *see, e.g.*, 18 U.S.C. § 2721 (restricting release of SSNs from motor vehicle records). Some States also recognize a constitutional right barring the government from disclosing SSNs without consent. *See, e.g.*, *280 *State ex rel. Beacon Journal Publ'g Co. v. City of Akron*, 70 Ohio St.3d 605, 640 N.E.2d 164, 169 (1994). Although not dispositive, these practices indicate a broad consensus that SSNs' public disclosure should be strictly curtailed.

Given the serious privacy concerns and potential harm stemming from SSN dissemination, Virginia's asserted interest in protecting individual privacy by limiting SSNs' public disclosure may certainly constitute "a state interest of the highest order." *Daily Mail*, 443 U.S. at 103, 99 S.Ct. 2667. We need not ultimately decide that question, however, because our holding below regarding narrow-tailoring suffices to resolve the constitutional challenge. We discussed this issue merely to provide guidance to the district court fashioning injunctive relief on remand. *See Elm Grove Coal Co. v. Dir., O. W.C.P.*, 480 F.3d 278, 299 n. 20 (4th Cir.2007) ("We choose to address this discovery issue because it is likely to arise on remand."); *Charbonnages de France v. Smith*, 597 F.2d 406, 417 (4th Cir.1979) ("[I]t may be appropriate to address a few points presented on this appeal that, although not dispositive here, could arise as important issues on remand.").

2.

We next consider whether enforcing section 59.1–443.2 against Ostergren would be narrowly tailored to Virginia's asserted interest in preserving individual privacy by protecting SSNs from public disclosure. Supreme Court precedent imposes a stringent standard regarding narrow-tailoring. *Cox*

Broadcasting and its progeny indicate that punishing truthful publication of private information will almost never be narrowly tailored to safeguard privacy when the government itself released that information to the press. *See Cox Broad.*, 420 U.S. at 496, 95 S.Ct. 1029 ("Once true information is disclosed in public court documents open to public inspection, the press cannot be sanctioned for publishing it."); *Florida Star*, 491 U.S. at 534, 109 S.Ct. 2603 ("Where information is entrusted to the government, a less drastic means than punishing truthful publication almost always exists for guarding against the dissemination of private facts."). Even where disclosure to the press was accidental, *Florida Star* indicates that the press cannot be prevented from publishing the private information. In that case, B.J.F.'s identity was disclosed to the press accidentally despite the police department's policy against revealing rape victims' names. The Supreme Court nonetheless concluded that "[w]here ... the government has failed to police itself in disseminating information, it is clear under *Cox Broadcasting*, *Oklahoma Publishing*, and *Landmark Communications* that the imposition of damages against the press for its subsequent publication can hardly be said to be a narrowly tailored means of safeguarding anonymity." *Florida Star*, 491 U.S. at 538, 109 S.Ct. 2603.

In both *Cox Broadcasting* and *Florida Star*, the government disclosed private information to the press and thereafter sought to prevent media outlets from truthfully publishing that information. This case appears similar in that Virginia likewise disclosed public records containing private information to Ostergren and now seeks to prevent her from publishing them online. Because Virginia "failed to police itself in disseminating information," *Cox Broadcasting* and *Florida Star* suggest that preventing Ostergren from publishing those records could almost never be narrowly tailored. *Id.* According to their stringent standard, Ostergren could never be prohibited from publicizing SSN-containing Virginia land records she already lawfully obtained (including those posted *281 on her website),[FN13] and Virginia would need to redact all original land records available from courthouses (not merely digital copies available through secure remote access) before Ostergren could be prohibited from publishing SSN-containing Virginia land records she might later obtain.[FN14]

FN13. Whereas Ostergren posted online only about 30 records from various States, her testimony indicates she obtained thousands of other public records containing unredacted SSNs.

FN14. The district court was justifiably concerned about reaching this extreme conclusion. When Ostergren maintained that under *Cox Broadcasting* she could continue publicizing additional SSNs until Virginia finished redacting all original land records and digital copies, the court responded,

> [I]f I understand it correctly, under the relief you want, she can go to the record, she can take thousands or hundreds of thousands, whatever is there, and publish them, and if she thinks that 20 names have shock value, what do you think her attitude might be toward publishing thousands or hundreds of thousands?

J.A. 192. Ostergren replied,

> It is relief I want, and I wish I could tell you a principled way to make it narrower, but I can't think of one, and I think that the *Cox* court struck the balance between privacy and free speech in the context of public records, and the way that they struck the balance was to hold that when the Government makes something available, they are responsible for controlling the dissemination of information. They can't make someone else do it.

J.A. 193. The court responded again,

> [W]hat if accidentally the Social Security Administration, somebody went in and released all the Social Security numbers in the country? Are you saying that Congress couldn't come in with a statute and say, you can't replicate these things? What they would do is try to take the system that had gone wrong, fix what they can fix, knowing that there are people who have already gotten into the database that spilled accidentally, but knowing the damage is somewhat limited and saying we are going to stop it right here, and the way we're going to stop it is making it unlawful for you, anybody, to take this information that's been accidentally spilled and use it.

J.A. 193. We share the district court's concern and consider below how the instant case may be distinguished from *Cox Broadcasting* and *Florida Star* regarding narrow-tailoring.

Despite apparent similarities, however, the instant case also differs from *Cox Broadcasting* and *Florida Star* in two critical respects that warrant consideration because they impact our narrow-tailoring analysis. First, this case implicates a different conception of privacy—one predicated upon control of personal information rather than secrecy. Second, Virginia's knowledge about and practical control over the private information here differs significantly from the situations involved in *Cox Broadcasting* and *Florida Star*. Given these differences, this case requires a more nuanced analysis than that suggested above.[FN15] We consider each difference separately below and then discuss the proper narrow-tailoring analysis.

> FN15. We are distinguishing *Cox Broadcasting* and *Florida Star* merely with regard to the proper narrow-tailoring analysis, not with regard to whether the *Daily Mail* standard applies.

a.

Cox Broadcasting involved Georgia's tort of public disclosure of private information, in which "the plaintiff claims the right to be free from unwanted publicity about his private affairs, which, although wholly true, would be offensive to a person of ordinary sensibilities." *Cox Broad.*, 420 U.S. at 489, 95 S.Ct. 1029. This cause of action "define[s] and protect[s] an area of privacy free from unwanted publicity in the press." *Id.* at 491, 95 S.Ct. 1029. "[T]he gravamen of the claimed injury is the publication of information, whether true or not, the dissemination of which is embarrassing or otherwise painful to an *282 individual." *Id.* at 489, 95 S.Ct. 1029. *Florida Star* involved the same privacy interest. B.J.F. suffered emotional distress because the fact that she had been raped, information she had hoped to keep secret, had been widely publicized. *See Florida Star*, 491 U.S. at 528, 109 S.Ct. 2603 ("B.J.F. testified that she had suffered emotional distress from the publication of her name.").

Cox Broadcasting and *Florida Star* thus involved a particular conception of privacy whereby "private" matters are those one would prefer to keep hidden from other people because disclosure would be embarrassing or compromising.[FN16] *See Whalen v. Roe*, 429 U.S. 589, 598–99, 97 S.Ct. 869, 51 L.Ed.2d 64 (1977) (noting cases protecting "privacy" that involved "the individual interest in avoiding disclosure of personal matters"). Under this conception, one's privacy interest hinges upon whether information has been kept secret, and protecting privacy involves ensuring that people can keep personal matters secret or hidden from public scrutiny. *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 Cal. L.Rev. 1087, 1105 (2002) ("One of the most common understandings of privacy is that it constitutes the secrecy of certain matters. Under this view, privacy is violated by the public disclosure of previously concealed information."). Because this conception of privacy presupposes

secrecy, personal matters that have been publicly disclosed can no longer be considered private. *See id.* at 1107 ("[T]he view of privacy as secrecy often leads to the conclusion that once a fact is divulged in public, no matter how limited or narrow the disclosure, it can no longer remain private."). For example, the Supreme Court embraced this reasoning in Fourth Amendment cases indicating that one's "reasonable expectation of privacy" cannot encompass anything exposed to the public or third parties. *See California v. Greenwood*, 486 U.S. 35, 40, 108 S.Ct. 1625, 100 L.Ed.2d 30 (1988) (finding no reasonable expectation of privacy in garbage because "plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public"); *United States v. Miller*, 425 U.S. 435, 442, 96 S.Ct. 1619, 48 L.Ed.2d 71 (1976) (finding no reasonable expectation of privacy in personal financial documents held by banks because "the documents obtained, including financial statements and deposit slips, contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business").

> FN16. The Seventh Circuit has explored the human desire for secrecy about certain personal matters:
>
> > Even people who have nothing rationally to be ashamed of can be mortified by the publication of intimate details of their life. Most people in no wise deformed or disfigured would nevertheless be deeply upset if nude photographs of themselves were published in a newspaper or a book. They feel the same way about photographs of their sexual activities, however "normal," or about a narrative of those activities, or about having their medical records publicized. Although it is well known that every human being defecates, no adult human being in our society wants a newspaper to show a picture of him defecating. The desire for privacy illustrated by these examples is a mysterious but deep fact about human personality.
>
> *Haynes v. Alfred A. Knopf, Inc.*, 8 F.3d 1222, 1229 (7th Cir.1993).

The instant case involves a different conception of privacy not predicated upon secrecy. *Cox Broadcasting* and *Florida Star* addressed the privacy concern that disclosing certain personal matters (information one had hoped to keep secret) might cause embarrassment or reputational damage. But people do not feel embarrassed***283** when asked to provide their SSN; nor do they fear that their reputation will suffer when others find out that number. People worry only about how their SSN will be used—more specifically, about whether some unscrupulous person will steal their identity. The Fifth Circuit made this same observation:

> [A]n individual's informational privacy interest in his or her SSN is substantial. The privacy concern at issue is not, of course, that an individual will be embarrassed or compromised by the particular SSN that she has been assigned. Rather, the concern is that the simultaneous disclosure of an individual's name and confidential SSN exposes that individual to a heightened risk of identity theft and other forms of fraud.

Sherman v. U.S. Dep't of the Army, 244 F.3d 357, 365 (5th Cir.2001); *see also Nat'l Cable & Telecomms. Ass'n v. FCC*, 555 F.3d 996, 1001 (D.C.Cir.2009) ("[W]e do not agree that the interest in protecting customer privacy is confined to preventing embarrassment....") Accordingly, this case involves a particular conception of privacy whereby one does not mind publicity itself but nonetheless would prefer to control how personal information will be used or handled. Under this conception, privacy does not hinge upon secrecy but instead involves "the individual's *control* of information concerning his or her person." *Nat'l Cable & Telecomms. Ass'n*, 555 F.3d at 1001 (emphasis added and internal quotations omitted).

This difference affects our narrow-tailoring analysis because *Cox Broadcasting*'s holding stemmed from the conception of privacy predicated upon secrecy. The Supreme Court noted that Georgia's tort of public disclosure of private information provided no remedy where the disclosed information was already publicly available. *See* Restatement (Second) of Torts § 652D cmt. b ("There is no liability when the defendant merely gives further publicity to information about the plaintiff that is already public."). The Court thus concluded that "the interests in privacy fade when the information involved already appears on the public record." *Cox Broad.*, 420 U.S. at 494–95, 95 S.Ct. 1029. This makes sense where privacy hinges upon secrecy because publicly accessible information could not be considered private anymore and any emotional distress resulting from disclosure would likely have already occurred.[FN17] But the reasoning makes noticeably less sense where privacy hinges upon control. Whereas emotional distress resulting from disclosure occurs only once when one discovers the publicity, publicly accessible SSNs could be misused repeatedly over time until they become less easily accessed. Furthermore, because SSNs are more easily accessed online than in bound original land records, people worried about preventing identity theft (rather than embarrassment) would indeed have a considerable privacy interest against "merely giv[ing] further publicity." Restatement (Second) of Torts § 652D cmt. b.

> FN17. The emotional distress that a rape victim experiences because of public disclosure of her identity occurs the moment she discovers that others know her secret. The harm feared by someone whose SSN has been disclosed, however, does not occur upon disclosure but rather upon the misuse of that information.

[7] The Supreme Court employed similar reasoning in *United States Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 109 S.Ct. 1468, 103 L.Ed.2d 774 (1989). In that case, reporters filed requests under the Freedom of Information Act, 5 U.S.C. § 552, for criminal identification records, known as "rap sheets," that the Federal *284 Bureau of Investigation had created by collecting biographical data and criminal history found in different state and local public records. The government refused to disclose these rap sheets based on the statutory exception for "records or information compiled for law enforcement purposes ... the production of [which] ... could reasonably be expected to constitute an unwarranted invasion of personal privacy." 5 U.S.C. § 552(b)(7)(C). Arguing that this exception was inapplicable, the reporters reasoned that "[b]ecause events summarized in a rap sheet have been previously disclosed to the public ... [the] privacy interest in avoiding disclosure of a federal compilation of these events approaches zero." *Reporters Comm.*, 489 U.S. at 762–63, 109 S.Ct. 1468. The Supreme Court expressly rejected this "cramped notion of personal privacy" and expounded as follows:

> [T]he common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person. In an organized society, there are few facts that are not at one time or another divulged to another. Thus the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private.

Id. at 763, 109 S.Ct. 1468. The Court then observed that "there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information." *Id.* at 764, 109 S.Ct. 1468. In another case, the Court reiterated what this analysis makes clear: "An individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in

some form." *U.S. Dep't of Def. v. Fed. Labor Relations Auth.*, 510 U.S. 487, 500, 114 S.Ct. 1006, 127 L.Ed.2d 325 (1994).

b.

The instant case also differs in another respect from *Cox Broadcasting* and *Florida Star* regarding narrow-tailoring. There, the Supreme Court held that punishing truthful publication of private information was not narrowly tailored because the government could have initially refused to disclose that information to the press. This rationale assumes that the government could have easily prevented initial disclosure. *See Florida Star*, 491 U.S. at 538, 109 S.Ct. 2603 ("[W]here the government itself provides information to the media, it is most appropriate to assume that the government had, but failed to utilize, far more limited means of guarding against dissemination than the extreme step of punishing truthful speech."). That assumption does not fully apply in this case.

Both *Cox Broadcasting* and *Florida Star* involved situations in which a government employee created the document containing sensitive information that was later disclosed. Thus, initial disclosure could have been avoided by not recording the information or sealing the document from the outset. In *Florida Star*, the Court recognized that the police officer who prepared the incident report could have simply omitted B.J.F.'s name. *See id.* Likewise, in *Cox Broadcasting*, the government could have omitted the victim's name from its indictments or placed them under seal. *See Cox Broad.*, 420 U.S. at 496, 95 S.Ct. 1029 ("If there are privacy interests to be protected in judicial proceedings, the States must respond by means which avoid *285 public documentation or other exposure of private information.").

This appeal presents a quite different situation. For the most part, private attorneys (rather than the government) were responsible for creating real estate documents containing people's SSNs and then submitting those documents for recording in Virginia. The clerk of court could have inspected these documents before recording them and redacted any SSNs, but even this solution differs from *Cox Broadcasting* and *Florida Star*, where the government did not have to search for the sensitive information needing redaction. Given that every year hundreds of thousands of documents are submitted for recording in Virginia, inspecting each one would have been no small undertaking. Most importantly, however, attorneys began filing documents containing SSNs long before Virginia could have been expected to comprehend the current threat of identity theft. For this reason, we find inapplicable *Cox Broadcasting*'s observation that "[b]y placing the information in the public domain on official court records, the State must be presumed to have concluded that the public interest was thereby being served." 420 U.S. at 495, 95 S.Ct. 1029.

Virginia currently prohibits attorneys from submitting real estate documents for recording that contain unredacted SSNs. *See* Va.Code § 17.1–227. Given the historical circumstances, however, clerks of court still possess millions of land records, over three percent of which probably contain unredacted SSNs. Inspecting all these records to find and redact SSNs would be far more burdensome than sealing indictments and police reports revealing rape victims' identities. Moreover, clerks cannot place original land records under seal while completing such redaction because people must inspect them to verify who owns what during real estate transactions. *See* Va.Code § 17.1–208 (requiring that "any records and papers of every circuit court that are maintained by the clerk of the circuit court shall be open to inspection by any person"). Furthermore, regarding land records available through secure remote access, the parties agree that running software used for redacting SSNs costs about four cents per page and has a one to five percent error rate. Virginia thus faces considerable obstacles in avoiding initial disclosure of sensitive information that *Cox Broadcasting* and *Florida Star* did not have to consider. Such realities plainly must factor into our narrow-tailoring analysis.

c.

[8] The factual differences between this case and *Cox Broadcasting* and *Florida Star* suggest the need for a more nuanced analytical approach to the *Daily Mail* standard's narrow-tailoring requirement. The Supreme Court's recognition of different conceptions of privacy—one focused upon secrecy and incompatible with any disclosure, the other focused upon control and consistent with limited disclosure—and the unrealistic challenge of preserving total secrecy in this situation strongly suggest that Virginia should have more latitude to limit disclosure of land records containing unredacted SSNs than *Cox Broadcasting* and *Florida Star* allowed for protecting rape victims' anonymity. Specifically, the Court's First Amendment jurisprudence does not necessarily require that Virginia redact SSNs from all original land records maintained in courthouse archives before someone like Ostergren may be prevented from publishing them online.[FN18] Ostergren's website supports*286 this conclusion by recognizing the critical difference between original land records available from courthouses and digital land records available through secure remote access:

> FN18. Ostergren took the contrary position below, arguing that all original land records had to be redacted before Virginia could prevent Ostergren from publishing SSNs online. *See* J.A. 120 ("Well, I think that the constitutional argument would still be solid even if the records were not available online, because they are open to anyone who wishes to see them."). But suspending access to courthouse archives until Virginia completed such an enormous redaction effort—requiring manual inspection of over 200 million physical documents—seems impossible because people require access to land records for any real estate transaction.

> Once records are recorded at the courthouse, they become public (unless sealed by a judge) and anyone can get them. But shouldn't we all have to drive to the Courthouse to see them? Yes, but sadly that is not the case anymore. Legislators have kowtowed to special interests and in VA, they voted specifically to allow these records online.
>
> The Virginia Watchdog, http:// www. opcva. com/ watchdog/ RECORDS.html (last visited Apr. 26, 2010) (emphasis omitted); *see Reporters Comm.*, 489 U.S. at 764, 109 S.Ct. 1468 (noting "a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information").

This certainly does not mean, however, that enforcing section 59.1–443.2 against Ostergren would be constitutional. We cannot conclude that prohibiting Ostergren from posting public records online would be narrowly tailored to protecting individual privacy when Virginia currently makes those same records available through secure remote access without having redacted SSNs. The record reflects that 15 clerks of court have not finished redacting SSNs from their land records, which are nonetheless available online. Under *Cox Broadcasting* and its progeny, the First Amendment does not allow Virginia to punish Ostergren for posting its land records online without redacting SSNs when numerous clerks are doing precisely that.[FN19] *Cf. Florida Star*, 491 U.S. at 535, 109 S.Ct. 2603 ("[W]here the government has made certain information publicly available, it is highly anomalous to sanction persons other than the source of its release."). Virginia could curtail SSNs' public disclosure much more narrowly by directing clerks not to make land records available through secure remote access until after SSNs have been redacted.[FN20]

> FN19. For the same reason, Virginia could not punish Ostergren for publishing a SSN-containing land record that had accidentally been overlooked during its imperfect

redaction process—having a one to five percent error rate—unless Virginia had first corrected that error. Even then, we leave open whether under such circumstances the Due Process Clause would not preclude Virginia from enforcing section 59.1–443.2 without first giving Ostergren adequate notice that the error had been corrected.

FN20. Although suspending secure remote access until the redaction process has ended would certainly make enforcing section 59.1–443.2 against Ostergren more narrowly tailored, we leave open whether this safeguard alone would be adequate under the *Daily Mail* standard. Once a greater factual record has been developed on remand, the district court in fashioning injunctive relief should consider whether other safeguards are also constitutionally required. *See, e.g., Florida Star*, 491 U.S. at 534, 109 S.Ct. 2603 ("The government may classify certain information, establish and enforce procedures ensuring its redacted release, and extend a damages remedy against the government or its officials where the government's mishandling of sensitive information leads to its dissemination.").

In summary, Virginia's failure to redact SSNs before placing land records online *287 means that barring Ostergren's protected speech would not be narrowly tailored to Virginia's interest in protecting individual privacy. For this reason, we hold that enforcing section 59.1–443.2 against Ostergren for the Virginia land records posted on her website would violate the First Amendment. We thus affirm the district court's August 22, 2008, decision.

III.

[9] We next consider Ostergren's challenge to the district court's award of injunctive relief. "We review an order granting an injunction for an abuse of discretion, reviewing factual findings for clear error and legal conclusions de novo." *Muffley ex rel. NLRB v. Spartan Mining Co.*, 570 F.3d 534, 543 (4th Cir.2009). The court entered

> a permanent injunction ... against enforcement of Va.Code § 59.1–443.2 against any iteration of Ostergren's website, now or in the future, that simply republishes publicly obtainable documents containing unredacted SSNs of *Virginia legislators, Virginia Executive Officers or Clerks of Court* as part as [sic] an effort to reform Virginia law and practice respecting the publication of SSNs online.

Ostergren, 643 F.Supp.2d at 770 (emphasis added). Ostergren claims this relief was too limited. Because her website includes documents obtained from various States' websites revealing SSNs of non-Virginia public officials, Ostergren contends that the injunction should have reached not only "Virginia legislators, Virginia Executive Officers or Clerks of Court" but also other public officials anywhere in the United States. *Id.*

A.

When Ostergren raised this issue below during a hearing about the propriety and scope of injunctive relief, counsel for the Attorney General stated that section 59.1–443.2 did not reach non-Virginia public records and that, regardless, the Attorney General would not prosecute Ostergren for publishing such documents. Because the issue had never been disputed, even prior to litigation, the district court declined to decide the question because that would "become[ ] an advisory opinion." J.A. 301–02. In essence, the court concluded that Ostergren failed to provide a case or controversy sufficient to trigger federal judicial power. *See Richmond Med. Ctr. For Women v. Herring*, 570 F.3d 165, 172 (2009) ("Article III ... extends the jurisdiction of courts only to cases and controversies, thus precluding courts from issuing advisory opinions....").

[10] The precise issue the district court passed over was whether the First Amendment prohibits

Virginia from enforcing section 59.1–443.2 against Ostergren for publishing on her web-site public records that contain unredacted SSNs but were obtained from other States' websites. Before entertaining Ostergren's argument about this, we consider our own jurisdiction to decide that question. *See Friedman's, Inc. v. Dunlap*, 290 F.3d 191, 197 (4th Cir.2002) ("[T]he question of whether we are presented with a live case or controversy is a question we may raise *sua sponte*.").

[11][12][13] Article III gives federal courts jurisdiction only over "Cases" or "Controversies." U.S. Const. art. III, § 2, cl. 1. Our judicial power may be exercised only where " 'conflicting contentions of the parties ... present a real, substantial controversy between parties having adverse legal interests, a dispute definite and concrete, not hypothetical or abstract.' " *Miller v. Brown*, 462 F.3d 312, 316 (4th Cir.2006) (quoting *288*Babbitt v. United Farm Workers Nat'l Union*, 442 U.S. 289, 298, 99 S.Ct. 2301, 60 L.Ed.2d 895 (1979)). From this requirement courts developed the doctrine of ripeness. "[I]ts basic rationale is to prevent the courts, through avoidance of premature adjudication, from entangling themselves in abstract disagreements...." *Abbott Labs. v. Gardner*, 387 U.S. 136, 148, 87 S.Ct. 1507, 18 L.Ed.2d 681 (1967). We assess ripeness by "balanc[ing] the fitness of the issues for judicial decision with the hardship to the parties of withholding court consideration." *Miller*, 462 F.3d at 319 (internal quotations omitted). Because "[t]he doctrine of ripeness prevents judicial consideration of issues until a controversy is presented in clean-cut and concrete form," *id.* at 318–19 (internal quotations omitted), "problems such as the inadequacy of the record ... or ambiguity in the record ... will make a case unfit for adjudication on the merits," *Scott v. Pasadena Unified Sch. Dist.*, 306 F.3d 646, 662 (9th Cir.2002) (internal quotations omitted).

Ostergren developed almost no evidentiary record to inform our decision about the issue raised. The record does not indicate from which States' websites she obtained public records containing unredacted SSNs, whether those records had previously been publicly disclosed, or how these States protected SSNs from public disclosure. We have only a stipulation that her website "includes public records obtained from government websites in other states." J.A. 86. We cannot imagine how any court could decide the question now presented with such a paltry evidentiary record, particularly given the fact-intensive inquiry required by *Cox Broadcasting* and its progeny. Ostergren also failed to develop any legal theory explaining why our First Amendment analysis about Virginia's land records should also encompass public records from other States. Her attorney admitted at oral argument, "I have not found a satisfactory answer to that question." Finally, thus far the Attorney General does not believe that section 59.1–443.2 would reach non-Virginia public records, and seems opposed to prosecuting Ostergren for publishing such documents. In short, we have no evidence, no argument, and no underlying dispute for the thorny constitutional question that Ostergren has raised. We therefore also have no jurisdiction to decide that question. *See California Bankers Ass'n v. Shultz*, 416 U.S. 21, 64, 94 S.Ct. 1494, 39 L.Ed.2d 812 (1974) ("Passing upon the possible significance of the manifold provisions of a broad statute in advance of efforts to apply the separate provisions is analogous to rendering an advisory opinion upon a statute or a declaratory judgment upon a hypothetical case." (internal quotations omitted)).

B.

[14] Although we decline to consider whether the First Amendment prohibits Virginia from enforcing section 59.1–443.2 against Ostergren for publishing non-Virginia public records containing unredacted SSNs, that does not moot Ostergren's cross-appeal. We therefore proceed to consider whether the district court abused its discretion by entering a permanent injunction that protected only "republish[ing] publicly obtainable documents containing unredacted SSNs of Virginia legislators, Virginia Executive Officers or Clerks of Court as

part as [sic] an effort to reform Virginia law and practice respecting the publication of SSNs online." *Ostergren*, 643 F.Supp.2d at 770.

[15] While district courts have broad discretion when fashioning injunctive relief, their powers are not boundless. "Once a constitutional violation is found, a ***289** federal court is required to tailor the scope of the remedy to fit the nature and extent of the constitutional violation." *Dayton Bd. of Educ. v. Brinkman*, 433 U.S. 406, 420, 97 S.Ct. 2766, 53 L.Ed.2d 851 (1977) (internal quotations omitted); *see Missouri v. Jenkins*, 515 U.S. 70, 88, 115 S.Ct. 2038, 132 L.Ed.2d 63 (1995) ("[T]he nature of the ... remedy is to be determined by the nature and scope of the constitutional violation." (internal quotations omitted)). Because we found that enforcing section 59.1–443.2 against Ostergren for the Virginia land records posted on her website violated the First Amendment under *Cox Broadcasting* and its progeny, we must consider whether the district court's injunctive relief was tailored to fit that violation. We are mindful that "[w]hile a remedy must be narrowly tailored, that requirement does not operate to remove all discretion from the District Court in its construction of a remedial decree." *United States v. Paradise*, 480 U.S. 149, 185, 107 S.Ct. 1053, 94 L.Ed.2d 203 (1987).

The district court tried "to frame a remedial injunction that ... accommodate [s] the First Amendment rights of Ostergren and, at the same time, affords some protection to the innocent members of the public who have no control of the release of the public records containing their SSNs." *Ostergren*, 643 F.Supp.2d at 769. Although we commend the court's conscientious effort to find minimally disruptive equitable relief, we conclude that its injunction was not tailored "to fit the nature and extent of [Virginia's] constitutional violation." *Brinkman*, 433 U.S. at 420, 97 S.Ct. 2766 (internal quotations omitted). The following examples are illustrative.

First, the injunction does not protect Ostergren in publishing Virginia land records containing private individuals' SSNs. Under our First Amendment analysis, Ostergren's constitutional right to publish Virginia land records containing unredacted SSNs does not depend on the political status of people whose SSNs are compromised. Therefore, restricting injunctive relief to "the SSN-containing records of State legislators, State Executive Officers and Clerks of Court, those who actually can act to correct the problem," contradicts our First Amendment holding. *Id.* at 770. The district court said that this limitation "largely only ratifies Ostergren's current course of conduct and, as she herself stated, would not have a seriously deleterious effect on her public advocacy." *Id.* But these circumstances do not justify ignoring the First Amendment. Furthermore, the record shows that Ostergren's advocacy did involve private individuals' SSNs. In June 2008, the clerk of court for Pulaski County, Arkansas, refused to remove land records from the Internet pending SSN redaction until Ostergren published land records showing several prominent local citizens' SSNs.

Second, the injunction does not protect Ostergren in publishing Virginia land records that contain non-Virginia public officials' SSNs. FN21 Many non-Virginia public officials conduct real estate transactions in Virginia and may have private information exposed in Virginia land records. For example, the record reflects that Ostergren published a land record from Fairfax County, Virginia, that contains General Colin Powell's unredacted SSN. Nothing in our First Amendment analysis justifies ***290** treating these records differently from other Virginia land records. Thus, even allowing the distinction between public and private individuals, the injunctive relief still does not adequately remedy Virginia's constitutional violation.

> FN21. Conversely, the injunction protects Ostergren in publishing non-Virginia public records containing Virginia public officials' SSNs. As we have noted, however, the question of whether Virginia could enforce section 59.1–443.2 against Ostergren for publishing non-Virginia public records

containing unredacted SSNs was not ripe for judicial consideration. *See ante* at III.A.

For the reasons stated above, we conclude that the district court abused its discretion by not "tailor[ing] the scope of the remedy to fit the nature and extent of the constitutional violation." *Brinkman*, 433 U.S. at 420, 97 S.Ct. 2766 (internal quotations omitted); *see United States v. Delfino*, 510 F.3d 468, 470 (4th Cir.2007) ("A district court abuses its discretion when it ... fails to consider judicially recognized factors constraining its exercise of discretion...."). We thus reverse the district court's June 2, 2009, decision and remand for further proceedings consistent with this opinion.

IV.

We recognize that on remand the district court will require a more developed factual record to determine proper injunctive relief. This includes evidence about the status and effectiveness of Virginia's current redaction efforts. Depending on the scope of section 59.1–443.2, this may also include evidence about non-Virginia public records that Ostergren would publish on her website. Because our constitutional analysis turned on how Virginia has handled public records rather than on whose SSNs are being exposed, the district court should frame the injunctive relief accordingly. The court should also heed *Florida Star*'s warning "that the sensitivity and significance of the interests presented in clashes between First Amendment and privacy rights counsel relying on limited principles that sweep no more broadly than the appropriate context of the instant case." 491 U.S. at 533, 109 S.Ct. 2603.

AFFIRMED IN PART, REVERSED IN PART, AND REMANDED

DAVIS, Circuit Judge, concurring:

I am pleased to concur in the fine opinion of my good colleague. I write separately to elaborate my view of one issue, namely, the appropriate test for identifying and assessing in First Amendment cases the existence of "a state interest of the highest order."

When evaluating whether a state's asserted interest rises to the level shared by those of "the highest order," courts must consider and weigh heavily the state's expressed views and its conduct or they risk denuding First Amendment rights. In *Florida Star v. B.J.F.*, 491 U.S. 524, 537–38, 109 S.Ct. 2603, 105 L.Ed.2d 443 (1989), the Court explained that Florida's statute failed to further a state interest of the highest order for three reasons, the first of which was that the appellant obtained the identifying information in question from the government in consequence of official mishandling of the information. *Id.* at 538, 109 S.Ct. 2603. This factor, combined with the breadth and facial underinclusiveness of Florida's statute, led the Court to find "no such interest is satisfactorily served by imposing liability under [the statute] to appellant under the facts of this case." *Id.* at 541, 109 S.Ct. 2603.

Considering a state's view and its actual conduct is particularly important in First Amendment cases like this one, in which the Commonwealth, a party to the case, undertakes to punish an individual for re-publishing information initially published by the Commonwealth itself. In such cases, courts should not casually treat a "state interest of the highest order" synonymously with a judicially-noticeable, constitutionally-rooted, "compelling governmental interest," such as the eradication of racial discrimination. *See* Maj. Op. at 277. ***291** Rather, the state's dual role as publisher and re-publication punisher necessitates a more searching analysis of its involvement. For this reason, while I agree with the observation in the majority opinion that certain evolving "practices indicate a broad consensus that SSNs' public disclosure should be strictly curtailed," Maj. Op. at 280, where, as here, an individual state has not manifested its genuine embrace of that "consensus," then judicially-noticed facts do not trump the state's tangible actions, nor can they render the state's behavior an unimportant or minor

aspect of the proper analysis.

Thus, an analysis of a state's view and its actual conduct in furthering its asserted interest is imperative in striking the proper balance, under the First Amendment, between pursuit of "a state interest of the highest order," on the one hand, and, on the other hand, the state's efforts to restrict the exercise of constitutionally-protected expressive activity. This is not to say that "objective" data have no role to play in the analysis of a federal court's assessment of whether an asserted state interest rises to become one "of the highest order." *See* Maj. Op. at 277. But such a consideration should not, and must not, supplant a fact-intensive inquiry into the state's view and its actual conduct in furthering its asserted interest.[FN*]

FN* *Butterworth v. Smith*, 494 U.S. 624, 110 S.Ct. 1376, 108 L.Ed.2d 572 (1990), is not to the contrary. There, the Supreme Court held unconstitutional a Florida statute that prohibited a writer's disclosure of his own grand jury testimony. *Id.* at 626, 110 S.Ct. 1376. In so holding, the Court considered whether other states maintain such a rule and whether the Federal Rules prohibited the writer's actions. *Id.* at 634–35, 110 S.Ct. 1376. But of course, in *Butterworth*, the state *never* had control of the information in question: the writer's testimony. Thus, the Court had scant reason to consider the actions of the state in safeguarding the information because the state never controlled the information in the first place.

In sum, when a state seeks to punish a speaker for republishing state-published information, the state should be expected, in the words of a contemporary colloquialism, not simply to talk the talk, but to walk the walk, as well. The district court did not err in so concluding here.

C.A.4 (Va.),2010.
Ostergren v. Cuccinelli

615 F.3d 263, 38 Media L. Rep. 2442

END OF DOCUMENT

215

Supreme Court

*Regina (GC) *v* Commissioner of Police of the Metropolis (Liberty and another intervening)

Regina (C) *v* Same (Same intervening)

[2011] UKSC 21

2011 Jan 31; Feb 1; May 18

Lord Phillips of Worth Matravers PSC, Lord Judge CJ, Lord Rodger of Earlsferry, Baroness Hale of Richmond, Lord Brown of Eaton-under-Heywood, Lord Kerr of Tonaghmore, Lord Dyson JJSC

Police — Powers — Retention of evidence — Police taking fingerprints and DNA samples from suspects — Suspects subsequently acquitted or not proceeded against — Statutory provision permitting retention of biometric data after purpose for which taken fulfilled — Whether compatible with Convention right to respect for private life — National police policy to retain biometric data indefinitely except in exceptional circumstances — Police refusing to destroy suspects' fingerprint records and sample in accordance with policy — Whether policy incompatible with Convention right — Whether declaration of incompatibility to be granted — Police and Criminal Evidence Act 1984 (c 60), s 64(1A) (as inserted by Criminal Justice and Police Act 2001 (c 16), s 82(2) and amended by Serious Organised Crime and Police Act 2005 (c 15), ss 117(7), 118(4)(a)) — Human Rights Act 1998 (c 42), s 3, Sch 1, Pt I, art 8

The claimant in the first case was arrested on suspicion of common assault and his fingerprints and a DNA sample were taken. He was subsequently informed by the police that no further action would be taken against him. The claimant in the second case was arrested on suspicion of rape, harassment and fraud and his fingerprints and a DNA sample were taken. No further action was taken in respect of the harassment and fraud allegations and he was acquitted of rape. The claimants requested the police to destroy their fingerprints and DNA samples. The Commissioner of Police of the Metropolis refused their requests in accordance with guidelines issued by the Association of Chief Police Officers ("ACPO"), which provided that the discretion in section 64(1A) of the Police and Criminal Evidence Act 1984[1], as amended, to retain fingerprints or samples after they had fulfilled the purposes for which they had been taken, in order to be used, inter alia, for the prevention and detection of crime, should be exercised for an indefinite period save in exceptional circumstances. The claimants each sought judicial review of the commissioner's decisions, relying in particular on a decision of the European Court of Human Rights that the blanket and indiscriminate nature of the powers of retention under section 64(1A) and the ACPO guidelines was an unjustified interference with an individual's right to respect for his private life under article 8.1 of the Convention for the Protection of Human Rights and Fundamental Freedoms, as scheduled to the Human Rights Act 1998[2].

[1] Police and Criminal Evidence Act 1984, s 64(1A), as inserted and amended: see post, para 3.

[2] Human Rights Act 1998, s 3: see post, para 113.

Sch 1, Pt I, art 8: "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."

A The Divisional Court of the Queen's Bench Division, holding itself bound by an earlier decision of the House of Lords which conflicted with the decision of the European court, dismissed the claims but granted the claimants a certificate under section 12(1) of the Administration of Justice Act 1969 for appeal direct to the Supreme Court. On the hearing of the appeal, the court was informed that the Government had introduced a Bill containing legislative proposals aimed at achieving a system for the retention of biometric data which was compatible with
B article 8.

On the appeals—

Held, allowing the appeals, (1) that, in the light of the European court's decision, the indefinite retention of the claimants' data was an unjustified interference with their rights under article 8.1 of the Convention (post, paras 15, 53, 64, 74, 77, 103, 138).

S and Marper v United Kingdom (2008) 48 EHRR 1169, GC applied.

C *R (S) v Chief Constable of the South Yorkshire Police* [2004] 1 WLR 2196, HL(E) departed from.

(2) (Lord Rodger of Earlsferry and Lord Brown of Eaton-under-Heywood JJSC dissenting) that Parliament, in conferring a discretion on the police to retain biometric data under section 64(1A) of the 1984 Act, had not specified how the statutory purposes were to be fulfilled and was not to be taken to have intended that they should be achieved in a manner which was incompatible with article 8; that
D section 64(1A) permitted a policy which was less far reaching than the ACPO guidelines, was compatible with article 8 and, nevertheless, promoted the statutory purposes; that, therefore, it was possible to read and give effect to section 64(1A), in accordance with section 3 of the Human Rights Act 1998, in a way which was compatible with the Convention; that, since Parliament was already seised of the matter, it was neither just nor appropriate to make an order requiring a change in the legislative scheme within a specific period or for the destruction of data which it
E might be lawful to retain under the scheme which Parliament produced; and that, accordingly, the only appropriate order was a declaration that the present ACPO guidelines were unlawful because they were incompatible with the Convention (post, paras 24–27, 28, 35, 39, 42–44, 46, 48–49, 52, 53, 55, 57–60, 64, 65, 69–70, 72–73, 74, 80–81, 85–86, 88–92).

Per Lord Phillips of Worth Matravers PSC, Lord Judge CJ and Lord Dyson JSC. If Parliament does not produce revised guidelines within a reasonable time the
F claimants will be able to seek judicial review of the continuing retention of their data under the unlawful ACPO guidelines and their claims will be likely to succeed (post, paras 49, 53, 74).

Decision of the Divisional Court of the Queen's Bench Division [2010] EWHC 2225 (Admin); [2010] HRLR 870, DC reversed.

The following cases are referred to in the judgments:

G *Aston Cantlow and Wilmcote with Billesley Parochial Church Council v Wallbank* [2003] UKHL 37; [2004] 1 AC 546; [2003] 3 WLR 283; [2003] 3 All ER 1213, HL(E)

Attorney General v Antigua Times Ltd [1976] AC 16; [1975] 3 WLR 232; [1975] 3 All ER 81, PC

Attorney General's Reference (No 3 of 1999) [2001] 2 AC 91; [2001] 2 WLR 56; [2001] 1 All ER 577, HL(E)

H *Bellinger v Bellinger (Lord Chancellor intervening)* [2003] UKHL 21; [2003] 2 AC 467; [2003] 2 WLR 1174; [2003] 2 All ER 593, HL(E)

British Broadcasting Corpn, In re [2009] UKHL 34; [2010] 1 AC 145; [2009] 3 WLR 142; [2010] 1 All ER 235, HL(E)

Car Owners' Mutual Insurance Co Ltd v Treasurer of the Commonwealth of Australia [1970] AC 527; [1969] 3 WLR 374, PC

Doherty v Birmingham City Council (Secretary of State for Communities and Local Government intervening) [2008] UKHL 57; [2009] AC 367; [2008] 3 WLR 636; [2009] 1 All ER 653, HL(E)
Ghaidan v Godin-Mendoza [2004] UKHL 30; [2004] 2 AC 557; [2004] 3 WLR 113; [2004] 3 All ER 411, HL(E)
Greens and MT v United Kingdom (Application Nos 60041/08 and 60054/08) (unreported) given 23 November 2010, ECtHR
Julius v Oxford (Bishop of) (1880) 5 App Cas 214, HL(E)
Manchester City Council v Pinnock (Secretary of State for Communities and Local Government intervening) [2010] UKSC 45; [2010] 3 WLR 1441; [2011] PTSR 61; [2011] 1 All ER 285, SC(E)
Padfield v Minister of Agriculture, Fisheries and Food [1968] AC 997; [1968] 2 WLR 924; [1968] 1 All ER 694, HL(E)
R v Kansal (No 2) [2001] UKHL 62; [2002] 2 AC 69; [2001] 3 WLR 1562; [2002] 1 All ER 257, HL(E)
R (Hooper) v Secretary of State for Work and Pensions [2005] UKHL 29; [2005] 1 WLR 1681; [2006] 1 All ER 487, HL(E)
R (L) v Comr of Police of the Metropolis (Secretary of State for the Home Department intervening) [2009] UKSC 3; [2010] 1 AC 410; [2009] 3 WLR 1056; [2010] PTSR 245; [2010] 1 All ER 113, SC(E)
R (S) v Chief Constable of the South Yorkshire Police [2004] UKHL 39; [2004] 1 WLR 2196; [2004] 4 All ER 193, HL(E)
S (Minors) (Care Order: Implementation of Care Plan), In re [2002] UKHL 10; [2002] 2 AC 291; [2002] 2 WLR 720; [2002] 2 All ER 192, HL(E)
S and Marper v United Kingdom (2008) 48 EHRR 1169, GC
Sheldrake v Director of Public Prosecutions [2004] UKHL 43; [2005] 1 AC 264; [2004] 3 WLR 976; [2005] 1 All ER 237, HL(E)
Silver v United Kingdom (1983) 5 EHRR 347

The following additional cases were cited in argument:

Hirst v United Kingdom (No 2) (2005) 42 EHRR 849, GC
R (Anderson) v Secretary of State for the Home Department [2002] UKHL 46; [2003] 1 AC 837; [2002] 3 WLR 1800; [2002] 4 All ER 1089, HL(E)
R (Chester) v Secretary of State for Justice [2010] EWCA Civ 1439; [2011] HRLR 209, CA
R (F (A Child)) v Secretary of State for the Home Department (Lord Advocate intervening) [2010] UKSC 17; [2011] 1 AC 331; [2010] 2 WLR 992; [2010] 2 All ER 707, SC(E)
R (Hirst) v Secretary of State for the Home Department [2002] EWHC 602 (Admin); [2002] 1 WLR 2929
R (Wood) v Comr of Police of the Metropolis [2009] EWCA Civ 414; [2010] 1 WLR 123; [2009] 4 All ER 951, CA

APPEALS from the Divisional Court of the Queen's Bench Division

The claimants, GC and C, each appealed, with permission granted by the Supreme Court (Lord Rodger of Earlsferry, Baroness Hale of Richmond and Lord Clarke of Stone-cum-Ebony JJSC) on 24 November 2010 and pursuant to certificates granted by the Divisional Court of the Queen's Bench Division (Moses LJ and Wyn Williams J) under section 12 of the Administration of Justice Act 1969 that a sufficient case had been made out for appeals direct to the Supreme Court, from the decision of the Divisional Court on 16 July 2010 [2010] HRLR 870 dismissing their claims for judicial review of decisions of the Commissioner of Police of the Metropolis not to destroy fingerprints and DNA samples which that had been taken from them in

connection with the investigation of offences for which they had not subsequently been prosecuted, or of which the second claimant had been acquitted.

The Secretary of State for the Home Department appeared as an interested party. Liberty and the Equality and Human Rights Commission intervened in the appeal, the latter by way of written submissions only.

The facts are stated in the judgment of Lord Dyson JSC.

Michael Fordham QC and *Dan Squires* (instructed by *Public Law Solicitors, Birmingham*) for the claimant, C.

Stephen Cragg and *Azeem Suterwalla* (instructed by *Fisher Meredith LLP*) for the claimant, GC.

Lord Pannick QC and *Jason Beer* (instructed by the *Director of Legal Services, Metropolitan Police*) for the commissioner.

James Eadie QC and *Jonathan Moffett* (instructed by *Treasury Solicitor*) for the Secretary of State.

Karon Monaghan QC and *Helen Law* (instructed by *Solicitor, Liberty*) for the first intervener.

Alex Bailin QC and *Adam Saudell* (instructed by *Solicitor, Equality and Human Rights Commission*) for the second intervener.

The court took time for consideration.

18 May 2011. The following judgments were handed down.

Majority judgments on the appropriate relief

LORD DYSON JSC

1 Biometric data such as DNA samples, DNA profiles and fingerprints is of enormous value in the detection of crime. It sometimes enables the police to solve crimes of considerable antiquity. There can be no doubt that a national database containing the data of the entire population would lead to the conviction of persons who would otherwise escape justice. But such a database would be controversial. It is not permitted by our law. Parliament has, however, allowed the taking and retention of data from certain persons. The questions raised by these appeals are whose data may be retained and for how long.

2 Section 64 of the Police and Criminal Evidence Act 1984 ("PACE"), as originally enacted, provided:

> "(1) If— (a) fingerprints or samples are taken from a person in connection with the investigation of an offence; and (b) he is cleared of that offence, they must be destroyed as soon as is practicable after the conclusion of the proceedings."
>
> "(3) If— (a) fingerprints or samples are taken from a person in connection with the investigation of an offence; and (b) that person is not suspected of having committed the offence, they must be destroyed as soon as they have fulfilled the purpose for which they were taken."

3 Section 64(1A) of PACE was inserted by section 82 of the Criminal Justice and Police Act 2001. It is still in force. As amended by sections 117(7) and 118(4)(a) of the Serious Organised Crime and Police Act 2005 it provides:

"Where— (a) fingerprints, impressions of footwear or samples are taken from a person in connection with the investigation of an offence, and (b) subsection (3) below does not require them to be destroyed, the fingerprints, impressions of footwear or samples may be retained after they have fulfilled the purposes for which they were taken but shall not be used by any person except for purposes related to the prevention or detection of crime, the investigation of an offence, the conduct of a prosecution or the identification of a deceased person or of the person from whom a body part came."

4 It will be seen at once that section 64(1A) does not specify any time limit for the retention of the data or any procedure to regulate its destruction. These are matters which are addressed in guidelines issued by the Association of Chief Police Officers ("the ACPO guidelines") entitled *Exceptional Case Procedure for Removal of DNA, Fingerprints and PNC Records* and published on 16 March 2006. So far as is material, these provide:

"it is important that national consistency is achieved when considering the removal of such records. Chief Officers have the discretion to authorise the deletion of any specific data entry on the [Police National Database] 'owned' by them. They are also responsible for the authorisation of the destruction of DNA and fingerprints associated with that specific entry. It is suggested that this discretion should only be exercised in exceptional cases . . . Exceptional cases will by definition be rare. They might include cases where the original arrest or sampling was found to be unlawful. Additionally, where it is established beyond doubt that no offence existed, that might, having regard to all the circumstances, be viewed as an exceptional circumstance."

5 In *R (S) v Chief Constable of the South Yorkshire Police*; *R (Marper) v Chief Constable of the South Yorkshire Police* [2004] 1 WLR 2196 ("*Marper UK*") the claimants sought judicial review of the retention by the police of their fingerprints and DNA samples on the grounds inter alia that it was incompatible with article 8 of the European Convention on Human Rights ("ECHR"). The majority of the House of Lords held that the retention did not constitute an interference with the claimants' article 8 rights, but they unanimously held that any interference was justified under article 8.2.

6 The European Court of Human Rights ("ECtHR") disagreed: see its decision in *S and Marper v United Kingdom* (2008) 48 EHRR 1169 ("*Marper ECtHR*"). In considering whether retention of data in accordance with the ACPO guidelines was proportionate and struck a fair balance between the competing public and private interests, the court said, at para 119:

"In this respect, the court is struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken—and retained—from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time-limited; the material is retained indefinitely whatever the nature or

seriousness of the offence of which the person was suspected. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the nationwide database or the materials destroyed; in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances."

The court concluded, at para 125:

"that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent state has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society."

7 On 16 December 2008, the Secretary of the State for the Home Department announced the Government's preliminary response to the ECtHR decision. The data of children under the age of 10 would be removed from the database immediately and the Government would issue a White Paper and consult on "bringing greater flexibility and fairness into the system by stepping down some individuals over time—a differentiated approach, possibly based on age, or on risk, or on the nature of the offences involved".

8 The White Paper, *Keeping the Right People on the DNA Database*, was published on 7 May 2009. It contained a series of proposals for the retention of data, the details of which are immaterial for present purposes.

9 On 28 July 2009, ACPO's Director of Information wrote to all chief constables (including the respondent commissioner) saying that the final draft for publication of new guidelines was not expected to take effect until 2010 and that until that time "the current retention policy on fingerprints and DNA remains unchanged".

10 On 11 November 2009, after the consultation period had ended, the Secretary of State made a written ministerial statement outlining a revised set of proposals. Again, the details are not material. It was decided to include these proposals in the Crime and Security Act 2010 which had its first reading on 19 November 2009. The 2010 Act received the Royal Assent on 8 April 2010, but the relevant provisions (sections 14, 22 and 23) have not been brought into effect. Section 23 provides that the Secretary of State must make arrangements for a National DNA Database Strategy Board ("Database Board") to oversee the operation of the National DNA Database (section 23(1)); the Database Board must issue guidance about the immediate destruction of DNA samples and DNA profiles which are or may be retained under PACE (section 23(2)); and any chief officer of a police force in England and Wales must act in accordance with any such guidance issued: section 23(3).

11 The Coalition Government stated in the Queen's Speech on 25 May 2010 that it intended to seek amendment of the 2010 Act by bringing

221

forward legislative proposals (in Chapter 1 of Part 1 of the Protection of Freedoms Bill) along the lines of the Scottish system. This system permits retention of data for no more than three years if the person is suspected (but not convicted) of certain sexual or violent offences, and permits an application to be made to a sheriff by a chief constable for an extension of that period (for a further period of not more than two years, although successive applications may be made): see sections 18 and 18A of the Criminal Procedure (Scotland) Act 1995, as inserted by sections 83(2) and 104 of the Police, Public Order and Criminal Justice (Scotland) Act 2006.

12 GC and C issued proceedings for judicial review of the retention of their data on the grounds that, in the light of *Marper ECtHR*, its retention was incompatible with their article 8 rights. Recognising that there was an irreconcilable conflict between *Marper UK* and *Marper ECtHR* and that the former decision was binding on it, the Divisional Court (Moses LJ and Wyn Williams J) [2010] HRLR 870 dismissed both judicial review challenges on 16 July 2010 and in both cases granted a certificate pursuant to section 12 of the Administration of Justice Act 1969 that the cases were appropriate for a leapfrog appeal to the Supreme Court.

13 The facts of these two cases can be stated briefly. On 20 December 2007, GC was arrested on suspicion of common assault on his girlfriend. He denied the offence. A DNA sample, fingerprints and photographs were taken after his arrest. On the same day, he was released on police bail without charge. Before the return date of 21 February 2008, he was informed that no further action would be taken. On 23 March 2009, GC's solicitors requested the destruction of the DNA sample, DNA profile and fingerprints. The commissioner refused to do so on the grounds that there were no exceptional circumstances within the meaning of the ACPO guidelines.

14 On 17 March 2009, C was arrested on suspicion of rape, harassment and fraud. His fingerprints and a DNA sample were taken. He denied the allegations saying that they had been fabricated by his ex-girlfriend and members of her family. No further action was taken by the police in respect of the harassment and fraud allegations. On 18 March 2009, he was charged with rape. On 5 May 2009 at the Crown Court at Woolwich, the prosecution offered no evidence and C was acquitted. C requested the destruction of the data and its deletion from the police database. On 12 November and again on 2 February 2010, the commissioner informed C that his case was not being treated as "exceptional" within the meaning of the ACPO guidelines and his request was refused.

The issue

15 It is common ground that, in the light of *Marper ECtHR* 48 EHRR 1169, the indefinite retention of the claimants' data is an interference with their rights to respect for private life protected by article 8 of the ECHR which, for the reasons given by the ECtHR, is not justified under article 8.2. It is agreed that *Marper UK* [2004] 1 WLR 2196 cannot stand. The issue that arises on these appeals is what remedy the court should grant in these circumstances.

16 On behalf of C, Mr Fordham QC submits that the court should grant a declaration under section 8(1) of the Human Rights Act 1998 ("HRA")

222

A that the retention of C's biometric data is unlawful. Section 8(1) provides that

> "In relation to any act (or proposed act) of a public authority which the court finds is (or would be) unlawful, it may grant such relief or remedy, or make such order, within its powers as it considers just and appropriate."

B He seeks no other relief.

17 On behalf of GC, Mr Cragg seeks an order quashing the ACPO guidelines and a reconsideration of the retention of GC's data within 28 days.

18 The primary submission of Lord Pannick QC (on behalf of the Commissioner of Police of the Metropolis) is that the correct remedy is to C grant a declaration of incompatibility under section 4 of the HRA. The primary submission of Mr Eadie QC (on behalf of the Secretary of State) is that, although there is no fundamental objection to a declaration of incompatibility, it is not necessary to grant one.

The arguments in support of a declaration of incompatibility

D 19 Section 6 of the HRA provides:

> "(1) It is unlawful for a public authority to act in a way which is incompatible with a Convention right.
>
> "(2) Subsection (1) does not apply to an act if— (a) as the result of one or more provisions of primary legislation, the authority could not have acted differently; or (b) in the case of one or more provisions of, or made E under, primary legislation which cannot be read or given effect in a way which is compatible with the Convention rights, the authority was acting so as to give effect to or enforce those provisions."

20 In summary, Lord Pannick and Mr Eadie say that it is not possible to read or give effect to section 64(1A) of PACE in a way which is consistent with *Marper ECtHR*. They accept that section 64(1A) confers a F discretionary power on the police to retain the data obtained from a suspect in connection with the investigation of an offence. That is why they concede that section 6(2)(a) of the HRA is not in play. But they say that it is a power which, save in exceptional circumstances, *must* be exercised so as to retain the data indefinitely in all cases. Section 64(1A) cannot, therefore, be read or given effect so as to permit the power to be exercised proportionately in the way described in *Marper ECtHR*. The hands of the police are tied by G section 64(1A) and that position is faithfully reflected in the ACPO guidelines.

21 Two arguments are advanced in support of this submission. The first (and principal) argument is that to interpret section 64(1A) as requiring police authorities to comply with article 8 would defeat the statutory purpose of establishing a scheme for the protection of the public interest free from the limits and protections required by article 8. It would rewrite the H statutory provision in a manner inconsistent with a fundamental feature of the legislative scheme which is that, instead of being destroyed, data taken from *all* suspects shall be retained *indefinitely*. It is this feature of the scheme which leads Lord Rodger of Earlsferry JSC to invoke authorities such as *Padfield v Minister of Agriculture, Fisheries and Food* [1968] AC 997.

223

Parliament intended that the discretion conferred by section 64(1A) should be exercised to promote the statutory policy and object that data taken from *all* suspects in connection with the investigation of an offence should be retained *indefinitely*. Accordingly, any exercise of the discretion conferred by section 64(1A) which does not meet this statutory policy and object would frustrate the intention of Parliament.

22 The second argument is that the nature of the changes to the ACPO guidelines that would be required in order to make them compatible with the ECHR is such that, for reasons of institutional competence and democratic accountability, these should be left to Parliament to make. The choice of compatible scheme involves a difficult and sensitive balancing of the interests of the general community against the rights of the individual and a number of different schemes would be compatible. Neither the police nor the court (in the event of a judicial review challenge to the scheme devised by the police) is equipped to make the necessary policy choices. Thus, for example, only Parliament is constitutionally and institutionally competent to decide whether to adopt the Scottish model in preference to the 2010 Act model.

Discussion

The first argument

23 This argument is based on the premise that it was the intention of Parliament that, save in exceptional cases, the data taken from *all* suspects in connection with the investigation of an offence should be retained *indefinitely*. It goes without saying that, if that premise is correct, section 64(1A) of PACE can only be interpreted as conferring a discretion which *must* be exercised so as to give effect to that intention. The conclusion necessarily follows from the premise. On that hypothesis, a purposive interpretation of the statute inevitably leads to the conclusion that the first argument is correct.

24 But I do not accept the premise. It is uncontroversial that Parliament intended (i) to abrogate section 64(1) of PACE and remove the obligation to destroy data as soon as practicable after the conclusion of the proceedings if the suspect is cleared of the offence; (ii) to create a scheme for the retention of the data taken from a suspect, whether or not he is cleared of the offence and whether or not he is even prosecuted; and (iii) that the data was to be retained so that it might be used "for purposes related to the prevention or detection of crime, the investigation of an offence, the conduct of a prosecution or the identification of a deceased person or of the person from whom a body part came" (to use the language of section 64(1A)). I shall refer to these purposes as "the statutory purposes". It is also clear that, in order to promote the statutory purposes, Parliament must have intended that an extended, even a greatly extended, database should be created. But in my view that is as far as it goes. To argue from the premise that Parliament intended that a greatly extended database should be created to the conclusion that it intended that, save in exceptional circumstances, the data should be retained indefinitely in all cases is a non sequitur.

25 Parliament did not prescribe the essential elements of the scheme by which the statutory purposes were to be promoted. That task was entrusted to the police, no doubt with the assistance of the Secretary of State. If it had

been intended to require a scheme whose essential elements included an obligation that, save in exceptional circumstances, the data lawfully obtained from *all* suspects should be retained *indefinitely*, that could easily have been expressly stated in the statute. If that had been intended, surely section 64(1A) would have said in terms that, save in exceptional circumstances, the fingerprints and samples taken "shall in every case be retained indefinitely after they have fulfilled the purpose for which they were taken". This would have been the obvious way of expressing that intention. The grant of an apparently unfettered discretion (signalled by the unqualified use of the word "may") was certainly not the obvious way of expressing that intention. The natural meaning of the word "may" is permissive, not mandatory.

26 As I have said, it is clear that Parliament intended to get rid of the requirement to destroy data after it has served its immediate purpose and to permit the retention of data in order to fulfil the statutory purposes. But the statute is silent as to how the statutory purposes are to be fulfilled. There is no reason to suppose that Parliament must have intended that this should be achieved in a disproportionate way so as to be incompatible with the ECHR. Lord Rodger JSC suggests that Mr Fordham's argument entails the proposition that under section 64(1A) the police were free to do what they liked and that the subsection contains nothing to delimit the exercise of their discretion. I agree that, if this is the effect of Mr Fordham's argument, it would cast doubt as to its correctness. But section 64(1A) clearly delimits the exercise of the discretion. It must be exercised to enable the data to be used for the statutory purposes. I would add that the discretion must be exercised in a way which is proportionate and rationally connected to the achievement of these purposes. Thus, for example, the police could not exercise the power to retain the data only of those suspected of minor offences; or only of serious offences of a particular type; or only of suspects of a certain age or gender; or only for a short period. But it is possible to exercise the discretion in a rational and proportionate manner which respects and fulfils the statutory purpose and does not involve the indefinite retention of data taken from all suspects, regardless of their age and the nature of the alleged offence.

27 The commissioner and the Secretary of State assert that a fundamental feature (possibly *the* fundamental feature) of section 64(1A) is that data should be retained for use from all suspects indefinitely. But, although expressed in different words, this is the same as the premise argument that I have already rejected. For the reasons I have given for rejecting that argument, it is not possible to extract this fundamental feature from the statute, whether one looks at its language alone or in the context of the mischief which it was intended to cure. In my view, the fundamental feature of section 64(1A) is that it gives the police the power to retain and use data from suspects for the stated statutory purposes of preventing crime, investigation of offences and the conduct of prosecutions. But that does not justify a blanket or disproportionate practice. Neither indefinite retention nor indiscriminate retention can properly be said to be fundamental features of section 64(1A).

28 As I have said, following the judgment of the ECtHR the Secretary of State for the Home Department took steps to take the DNA of children under the age of ten off the database. If the meaning of section 64(1A) is

that, save in exceptional cases, there is a duty to retain samples taken from all suspects indefinitely, then surely this amendment to the ACPO guidelines was ultra vires section 64(1A). That is not, however, suggested by Lord Pannick or Mr Eadie. It seems to me that, once it is accepted that section 64(1A) permits a scheme which does not insist on the indefinite retention of data in all cases, then the extreme position advocated by the commissioner and the Secretary of State cannot be maintained. So what did Parliament intend if it was not a scheme of indefinite retention in all cases? The obvious answer is a proportionate scheme which gives effect to the statutory purposes and is compatible with the ECHR. The fact that it is possible to create a number of different schemes all of which would meet these criteria does not matter. Section 64(1A) gives a power. Powers can often be lawfully exercised in different ways.

29 The commissioner and the Secretary of State seek support for the first argument from two sources. The first is the Explanatory Notes to the 2001 Act which explained at para 210:

> "An additional measure has been included to allow all fingerprints and DNA samples lawfully taken from suspects during the course of an investigation to be retained and used for the purposes of prevention and detection of crime and the prosecution of offences. This arises from the decisions of the Court of Appeal (Criminal Division) in *R v Weir* and *R v B (Attorney General's Reference No 3/199)* May 2000. These raised the issue of whether the law relating to the retention and use of DNA samples on acquittal should be changed. In these two cases compelling DNA evidence that linked one suspect to a rape and the other to a murder could not be used and neither could be convicted. This was because at the time the matches were made both defendants had either been acquitted or a decision made not to proceed with the offences for which the DNA profiles were taken. Currently section 64 of PACE specifies that where a person is not prosecuted or is acquitted of the offence the sample must be destroyed and the information derived from it can not be used. The subsequent decision of the House of Lords overturned the ruling of the Court of Appeal. The House of Lords ruled that where a DNA sample fell to be destroyed but had not been, although section 64 of PACE prohibited its use in the investigation of any other offence, it did not make evidence obtained as a failure to comply with that prohibition inadmissible, but left it to the discretion of the trial judge. The Act removes the requirement of destruction and provides that fingerprints and samples lawfully taken on suspicion of involvement in an offence or under the Terrorism Act can be used in the investigation of other offences. This new measure will bring the provisions of PACE for dealing with fingerprint and DNA evidence in line with other forms of evidence."

30 But this does not advance matters. It shows that Parliament intended to remove "the requirement of destruction" of data and that "fingerprints and samples lawfully taken on suspicion of involvement in an offence . . . can be used in the investigation of other offences". But that sheds no light on whether it was intended that there should be a policy of blanket indefinite retention. The commissioner and the Secretary of State draw attention to the words "an additional measure has been included to allow *all* [data] . . . to be retained" (emphasis added). But in my view this is an insufficient

226

A foundation on which to base a conclusion that the true meaning of section 64(1A) is that, save in exceptional circumstances, biometric data must be retained indefinitely in all cases. Even if "all" means all data taken from all suspects, the Explanatory Notes do not say that data must be retained in all cases, still less do they say anything about how long the data must or may be kept. There is no indication in the notes that Parliament B intended all material to be kept indefinitely even if it was not necessary to do so in an individual case within the meaning of article 8.2 of the ECHR.

31 The second source is certain passages in speeches of the House of Lords in *Marper UK* [2004] 1 WLR 2196. The issue there was whether section 64(1A) and the ACPO guidelines were compatible with article 8 and 14 of the ECHR: see para 6 of the speech of Lord Steyn. At para 2, Lord Steyn said: "But as a matter of policy it is a high priority that police forces C should expand the use of such evidence where possible and practicable." But that is a statement at a high level of generality. Lord Steyn was not purporting to define the statutory purpose with any precision.

32 At para 39 Lord Steyn addressed the submission on behalf of the claimants that the legislative aim (of assisting in the investigation of crimes in the future) could be achieved by less intrusive means. He considered the D conclusion of Sedley LJ in the Court of Appeal that the degree of suspicion should be considered in individual cases before a decision was made whether or not to retain the data. He rejected this suggestion saying:

> "this would not confer the benefits of a greatly expanded database and would involve the police in interminable and invidious disputes (subject to judicial review of individual decisions) about offences of which the E individual had been acquitted."

I have already accepted that Parliament intended that the exercise of the section 64(1A) power should lead to a "greatly expanded database" and that Lord Steyn was rejecting the idea that the scheme contemplated by section 64(1A) should involve assessment of the degree of suspicion on a case by case basis. But he was not saying that, subject to exceptional F circumstances, section 64(1A) required the introduction of a scheme under which the data taken from all suspects would be retained indefinitely, since any other interpretation would undermine the statutory purpose.

33 At para 78, Baroness Hale of Richmond said that the whole community (as well as the individuals whose samples are collected)

> "benefits from there being as large a database as it is possible to have. The present system is designed to allow the collection of as many samples G as possible and to retain as much as possible of what it has."

That is undoubtedly true. But the "system" included the ACPO guidelines. It was, therefore, not contentious that the "system" was designed to catch and retain as many samples as possible. Moreover, leaving ECHR issues aside, section 64(1A) does *allow* the collection and retention of as many samples as possible. Baroness Hale was not, however, saying that H section 64(1A) *required* the collection and retention of as many samples as possible. Similarly, at para 88 Lord Brown of Eaton-under-Heywood said that the benefits of the "larger database brought about by the now impugned amendment to PACE" were manifest. The more complete the database, the better the chance of detecting criminals and of deterring future crime.

227

But here too, Lord Brown was not considering the question whether section 64(1A) conferred a power which, save in exceptional circumstances, could only be exercised by requiring the retention of the data taken from all suspects indefinitely. The question whether, leaving ECHR issues aside, section 64(1A) required the retention of the data taken from all suspects indefinitely was not in issue in *Marper UK*.

34 The focus of the argument in *Marper UK* was on whether section 64(1A) and the ACPO guidelines were compatible with the ECHR. In particular, it was on whether article 8.1 was engaged and whether the ACPO scheme was justified under article 8.2. The context of the observations relied on to support the first argument was the practice of the police, save in exceptional cases, to retain all data indefinitely. There was no debate on whether, if article 8.1 was engaged and the ACPO guidelines could not be justified under article 8.2, section 64(1A) could be read and given effect in a way compatible with the ECHR. So I reject the submission that *Marper UK* provides support for the submission that underpins the first argument, namely that it was the intention of Parliament that, save in exceptional cases, the data of *all* suspects should be retained *indefinitely*.

35 In my view, section 64(1A) permits a policy which (i) is less far reaching than the ACPO guidelines; (ii) is compatible with article 8 of the ECHR; and (iii) nevertheless, promotes the statutory purposes. Those purposes can be achieved by a proportionate scheme. It is possible to read and give effect to section 64(1A) in a way which is compatible with the ECHR and section 6(2)(b) of the HRA cannot be invoked to defeat the claim that the ACPO guidelines are unlawful by reason of section 6(1) of the HRA. For the reasons that I have given, to interpret section 64(1A) compatibly with article 8 does not impermissibly cross the line where, to use the words of Lord Bingham of Cornhill in *Sheldrake v Director of Public Prosecutions* [2005] 1 AC 264, para 28, it

> "would be incompatible with the underlying thrust of the legislation, or would not go with the grain of it, or would call for legislative deliberation, or would change the substance of a provision completely, or would remove its pith and substance, or would violate a cardinal principle of the legislation."

36 This conclusion is consistent with the decision in *R (L) v Comr of Police of the Metropolis (Secretary of State for the Home Department intervening)* [2010] 1 AC 410. The claimant was employed by an agency providing staff for schools. The agency required her to apply under section 115(1) of the Police Act 1997 for an enhanced criminal record certificate giving the prescribed details of every relevant matter relating to her which was recorded in central records, since she was a prospective employee who was being considered for a position involving regularly being involved with persons under the age of 18. Section 115(7) provided that, before issuing a certificate, the Secretary of State shall request the chief police officer of every relevant police force "to provide any information which, in the chief officer's opinion— (a) might be relevant for the purpose described in the statement under subsection (2), and (b) ought to be included in the certificate". The Commissioner of Police of the Metropolis disclosed certain information about the claimant which was included in the certificate.

A She sought judicial review of the decision to disclose the information on the ground that her article 8 rights had been violated.

37 On behalf of the Secretary of State, it was submitted that the words "any information" and "ought to be included" in section 115(7) showed that Parliament intended widespread disclosure of relevant material and a narrow exception. This interpretation was supported by the protective purpose of the legislation: see p 416G. That was the practice under the relevant police guidelines.

38 It is true that there was no issue in that case about section 6(2) of the HRA. That is why the analogy cannot be pressed too far. But in essence it was being argued in the context of article 8.2 of the ECHR that it was a fundamental feature of the Police Act 1997 that all relevant information could (and should) be disclosed in a criminal record certificate, since anything less would defeat the fundamental protective purpose of the statute. These submissions are similar to those advanced in the present case. But they were rejected. Despite the protective purpose of the legislation and the use of the word "any", at para 44, Lord Hope of Craighead DPSC said that the words "ought to be included" should be read and given effect in a way that was compatible with the applicant's article 8 rights. At para 81, Lord Neuberger of Abbotsbury MR adopted a broad interpretation of section 115(7)(b) and said that, in deciding whether the information ought to be included, there would be a number of different, sometimes competing, factors to weigh up.

39 For all these reasons, I would reject the first argument advanced on behalf of the commissioner and the Secretary of State.

The second argument

40 The second argument is that Parliament could not have intended to entrust the creation of a detailed scheme pursuant to section 64(1A) to the police (with or without the assistance of the Secretary of State) subject only to the judicial review jurisdiction of the court. It is said that the creation of guidelines for the exercise of the section 64(1A) power is a matter for Parliament alone and that it could not have been intended that section 64(1A) should grant a broad discretion to the police such as is contended for by Mr Fordham. This is because the context involves high policy, balancing the public interest in the effective detection, prosecution and prevention of crime against individual freedoms. It is a matter of political controversy, as evidenced by the different policy solutions of the previous and present Government. There are choices to be made between a variety of compatible legislative schemes. These choices are for Parliament alone. The police are in no position, constitutionally or institutionally, to choose between them.

41 It is important to note the scope of this argument. It is not that Parliament could not have granted the police a discretionary power to retain data otherwise than on a blanket indefinite basis. If it had wished to grant such a power to the police, Parliament obviously could have done so. Rather, the argument is that the constitutional and institutional limits on the competence of the police are such that Parliament could not have intended to grant such a power to them.

42 I cannot accept this argument. No question of constitutional competence arises here. Parliament is entitled to give the police the power to create a scheme. No doubt it would have envisaged that a national scheme

would be produced such as the ACPO guidelines. The Secretary of State is accountable to Parliament for the scheme so that the democratic principle is preserved.

43 There are circumstances in which institutional competence is a factor in the court's deciding the extent to which it should pay "deference" to a decision of the executive and allow a discretionary area of judgment. But we are not concerned with the court's judicial review jurisdiction in the present context. We are concerned with a question of statutory interpretation. There is no reason in principle why the police (together with the Secretary of State) should be less well equipped than Parliament to create guidelines for the exercise of the section 64(1A) power. In creating a proportionate scheme, they have to strike a balance. That is inherent in any exercise of this kind, whether it is performed by the executive or Parliament. The police guidelines that were in play in *R (L) v Comr of Police of the Metropolis* were not the product of work by Parliament. Policy and guidance documents of this kind, often in areas of acute sensitivity, are frequently created by the executive. Provided that they fulfil the purposes of the enabling statute, they are valid and enforceable.

44 In my view, the fact that difficult decisions would have to be made in producing guidelines for the exercise of the section 64(1A) power is not a sufficient reason for concluding that Parliament could not have intended to give the power to produce them to the police and the Secretary of State.

What relief, if any, should be granted?

The biometric data

45 In deciding what relief to grant, it is important to have regard to the present state of play. As previously stated, Chapter 1 of Part 1 of the Protection of Freedoms Bill includes proposals along the lines of the Scottish model. The history of the varying responses to *Marper ECtHR* 48 EHRR 1169 shows that it is not certain that it will be enacted. But we were told by Mr Eadie that it is the present intention of the Government to bring the legislation into force later this year. In shaping the appropriate relief in the present case, I consider that it is right to proceed on the basis that this is likely to happen, although not certain to do so.

46 In these circumstances, in my view it is appropriate to grant a declaration that the present ACPO guidelines (amended as they have been to exclude children under the age of 10), are unlawful because, as clearly demonstrated by *Marper ECtHR*, they are incompatible with the ECHR. It is important that, in such an important and sensitive area as the retention of biometric data by the police, the court reflects its decision by making a formal order to declare what it considers to be the true legal position. But it is not necessary to go further. Section 8(1) of the HRA gives the court a wide discretion to grant such relief or remedy within its powers as it considers just and appropriate. Since Parliament is already seised of the matter, it is neither just nor appropriate to make an order requiring a change in the legislative scheme within a specific period.

47 The ECtHR has recently decided that, where one of its judgments raises issues of general public importance and sensitivity, in respect of which the national authorities enjoy a discretionary area of judgment, it may be appropriate to leave the national legislature a reasonable period of time to

230

address those issues: see *Greens and MT v United Kingdom* (Application Nos 60041/08 and 60054/08) (unreported) given 23 November 2010, paras 113–115. This is an obviously sensible approach. The legislature must be allowed a reasonable time in which to produce a lawful solution to a difficult problem.

48 Nor would it be just or appropriate to make an order for the destruction of data which it is possible (to put it no higher) it will be lawful to retain under the scheme which Parliament produces.

49 In these circumstances, the only order that should be made is to grant a declaration that the present ACPO guidelines (as amended) are unlawful. If Parliament does not produce revised guidelines within a reasonable time, then the claimants will be able to seek judicial review of the continuing retention of their data under the unlawful ACPO guidelines and their claims will be likely to succeed.

The photographs of GC

50 Mr Cragg raises a discrete issue about the photographs that were taken of GC when he was arrested. Section 64A of PACE confers a power to take, use and retain photographs of arrested persons who are not subsequently convicted of the offence for which they were arrested. In the application for judicial review, the issue of whether the retention of the photographs violated GC's article 8 rights was mentioned in what Moses LJ described, at para 40, as "a passing reference in the claim form and in paragraph 20 of the grounds". At para 43, Moses LJ said: "the issues of justification for their retention cannot now properly be considered where the commissioner has had no opportunity to give evidence as to justification."

51 Lord Pannick submits that, in view of the manner in which the issue was raised in the Divisional Court, the consequent absence of any evidence as to justification and the absence of any substantive judgment on the issue from the Divisional Court, the Supreme Court should express no opinion on this part of the appeal, but leave the matter to be determined if and when the point is properly raised in another case. I accept these submissions. I should also mention that Mr Fordham raises a discrete point about information held on the Police National Computer about C. This was the subject of two agreed issues which were dealt with by the Divisional Court at paras 24–26 and 46–47 of the judgment of Moses LJ. It is common ground that the retention of this information raises no separate issues from those raised by the retention of C's DNA material and his fingerprints.

Conclusion

52 For the reasons that I have given, I would allow the appeals and grant a declaration that the present ACPO guidelines are unlawful because they are incompatible with article 8 of the ECHR. I would grant no other relief.

LORD PHILLIPS OF WORTH MATRAVERS PSC

53 I agree with the judgment of Lord Dyson JSC. I have, however, a little that I would add to his reasoning.

54 Section 3 of the Human Rights Act 1998 ("the HRA") requires this court, in so far as it is possible to do so, to interpret legislation in a way

which is compatible with Convention rights. Sometimes this results in the court according to a statutory provision a meaning that conflicts with the natural meaning of a statutory provision: see *Ghaidan v Godin-Mendoza* [2004] 2 AC 557. In summarising the effect of that decision in *Sheldrake v Director of Public Prosecutions* [2005] 1 AC 264, para 28 Lord Bingham of Cornhill stated that the interpretative obligation under section 3 was very strong and far reaching and might require the court to depart from the legislative intention of Parliament.

55 This is not a case where the HRA requires the court to accord to a statutory provision a meaning which it does not naturally bear. There is no difficulty in giving section 64(1A) of PACE, set out in para 3 of Lord Dyson JSC's judgment ("section 64(1A)"), an interpretation which is compatible with article 8 of the Convention, as interpreted by the European Court of Human Rights in *S and Marper v United Kingdom* 48 EHRR 1169. The section gives a discretionary power to the police to retain samples taken from a person in connection with the investigation of an offence. Section 3 of the HRA imposes a duty on the police, as a public authority, in so far as it is possible to do so, to give effect to the power conferred on them in a way which is compatible with Convention rights. There is nothing in the wording of section 64(1A), giving it its natural meaning, which either requires or permits the police to exercise the power conferred on them in a manner which is incompatible with article 8.

56 In order to hold that section 64(1A) is incompatible with the Convention it is thus necessary to identify some matter, extrinsic to the wording of the section itself, that compels one to interpret the section as either requiring or permitting the police to exercise the power conferred on them in a manner incompatible with article 8. Such a matter needs to be extraordinarily cogent in order to overcome the effect of section 3 of the HRA. I have not been able to identify any such matter.

57 In *R (S) v Chief Constable of the South Yorkshire Police; R (Marper) v Chief Constable of the South Yorkshire Police* [2004] 1 WLR 2196 the House of Lords held, wrongly as the European Court of Human Rights was to rule, that in so far as section 64(1A) interfered with article 8 rights the interference was justified under article 8.2. In so far as Parliament considered the matter when enacting section 64(1A) it is likely to have taken the same view. Parliament may well have considered that the Convention did not require any restriction to be placed on the exercise of the power conferred by section 64(1A). It does not follow, however, that Parliament must be presumed to have intended that, if the Convention did require the power to be exercised subject to constraints, the police should none the less be required, or permitted, to disregard those constraints.

58 The effect of section 64(1A) was to reverse the requirement of the previous section 64 of PACE that fingerprints and samples should be destroyed when a suspect was cleared of an offence. The purpose of this reversal was plainly that the police should be permitted to establish a database of such material obtained from those suspected of criminal activity. I see no basis for concluding, however, that Parliament intended that the establishment and maintenance of this database should be untrammelled by any requirements that might be imposed by the Convention. While those requirements limit the circumstances in which material can be retained by

application of the familiar test of proportionality, they do not prohibit the maintenance of a database that satisfies that test.

59 Had Parliament foreseen that the Convention required restrictions on the power conferred by section 64(1A) the likelihood is that Parliament, guided by the executive, would itself have wished to define those restrictions rather than leaving them to be determined by executive action. That can be deduced from the fact that Parliament's reaction to the European court's ruling in *S and Marper v United Kingdom* 48 EHRR 1169 was to pass amending legislation and that the present Government intends to introduce an amending Bill. I do not consider, however, that it follows from this that one must interpret section 64(1A) as requiring the police to exercise the power conferred by that section in a manner which infringes the requirements of the Convention, or even as permitting the police to disregard those requirements.

60 For these additional reasons I can see no warrant for making a declaration of incompatibility, convenient though this might be, and concur in the order proposed by Lord Dyson JSC.

BARONESS HALE OF RICHMOND JSC

61 Whether and in what circumstances the police should be able to keep the DNA samples and profiles, fingerprints and photographs of people who have been arrested but not convicted is a deeply controversial question. The Government is promoting the Protection of Freedoms Bill which will adopt in England and Wales the present system in Scotland. This allows retention only for a limited period and in respect of certain crimes. It reflects a strong popular sentiment that the police should not be keeping such sensitive material relating to "innocent" people, even if they are only allowed to use it "for purposes related to the prevention or detection of crime, the investigation of an offence, the conduct of a prosecution": Police and Criminal Evidence Act 1984, section 64(1A), as inserted by the Criminal Justice and Police Act 2001, section 82. If the popular press is any guide to public opinion, the decision of the European Court of Human Rights in *S and Marper v United Kingdom* 48 EHRR 1169 is one which captures the public mood in Britain much more successfully than many of its other decisions.

62 Among the arguments marshalled against retaining the data are these: (a) The agencies of the state cannot be trusted to use such information only for the permitted purposes, nor can the state be trusted not to enlarge those purposes in future. DNA samples, in particular, might be put to many more controversial uses should the state feel so inclined. (b) Serious bodies have cast doubt upon the usefulness of retaining it even for the permitted purposes. Both the Human Genetics Commission (*Nothing to hide, nothing to fear? Balancing individual rights and the public interest in the governance and use of the national DNA Database*, November 2009) and the Nuffield Council on Bioethics (*The forensic use of bioinformation: ethical issues*, September 2007) suggest that the value of casting the net so wide has not yet been proved. (c) The Equality and Human Rights Commission argue, in their intervention in this case, that the premise on which such data are kept, that people who are arrested are more likely than the general population to be involved in future offending, is "unsustainable". (d) Liberty point out, in their intervention, that certain sections of the population, in particular men and people from the black and minority ethnic communities, run a

disproportionate risk of arrest and therefore of having their data taken and kept. This is a detriment with a discriminatory impact. (e) The detriment is the stigma, certainly felt and possibly perceived by others, involved in having one's data on the database. This stigma, together with wider concerns about potential misuse, is sufficient to outweigh the benefits in the detection and prosecution of crime.

63 Among the arguments marshalled in favour of retaining the data are these: (a) Those of a more trusting nature find it difficult to imagine that there is a serious risk that the agencies of the state will indeed misuse this information for more sinister purposes. The risk would in any event be much reduced if DNA samples were destroyed and only profiles, fingerprints and photographs retained. (b) As to their usefulness, the Chief Constable of the West Midlands gave evidence on 22 March 2011 to the House of Commons Public Bill Committee hearing on the Protection of Freedoms Bill that between 2 and 3 per cent of the 36,000 "hits" on the database would be lost if the proposals in the Bill became law. These may only be a small proportion of the total, but among the 1,000 or so crimes which would not be solved some would be very serious. (c) It is not clear that the underlying premise is indeed that people who have been arrested but not charged or convicted are more likely than the general population to commit crimes. After all, the Act also allows the police to keep data they have collected from people who have never been arrested, provided that they consent. The reality is that arrest gives the police the opportunity compulsorily to collect the data: it is not the reason why they do so. (d) The discriminatory impact of disproportionate arrest rates among male and black and minority ethnic members of the population could as logically be addressed by compiling a national database of everyone, rather than by restricting it to people involved in the criminal justice system. There is now a proliferation of national databases holding data on large sections of the population which data can be put to far more detrimental uses than this. (e) Any stigma felt or perceived is irrational, at least if the information is used for its permitted purposes. A person who might otherwise have been among "the usual suspects" arrested for a crime may be eliminated before he even gets to the police station. A person who is rightly arrested, prosecuted and convicted because a match is found does not deserve our sympathy. We should be concentrating on the quality of the scientific evidence as to sampling and matching rather than on the feelings of those whose samples have been kept. The feelings of the victims of crime are at least as important as the feelings of the criminals. They too have a human right to have their physical and mental integrity protected by the law, and it is in this context that DNA evidence, in particular, has proved most useful.

64 We are not called upon to resolve that debate in this case. It is common ground that the decision of the House of Lords in *R (S) v Chief Constable of the South Yorkshire Police; R (Marper) v Chief Constable of the South Yorkshire Police* [2004] 1 WLR 2196 ("*Marper UK*") cannot stand in the light of the decision of the European Court of Human Rights in *S and Marper v United Kingdom* 48 EHRR 1169. The only question is what we should do about it in this case. This is, as I understand it, a question governed by legal principle and the Human Rights Act 1998 and not by our particular preferences for how the United Kingdom should solve the problem. There are three broad options open to the court. (i) We could

234

A decide, in the light of the individual facts of the cases before us, whether the retention of data in each case is compatible with the claimant's Convention rights. If it is not, we could make declarations to that effect and even mandatory orders for the deletion and destruction of the data involved. (ii) We could declare that the current ACPO guidelines, approved in *Marper UK*, are unlawful, without determining what would be lawful in the cases
B before us. (iii) We could declare that section 64(1A) of PACE is incompatible with the Convention rights, thus leaving the current guidelines in place and everything done under them lawful until Parliament enacts a replacement either by primary legislation or under the "fast track" remedial procedure laid down in section 10 of the Human Rights Act 1998.

65 The choice between (i) or (ii), on the one hand, and (iii), on the other hand, depends upon the "difficult and important" question (see Lord Mance
C in *Doherty v Birmingham City Council (Secretary of State for Communities and Local Government intervening)* [2009] AC 367, para 141) of the meaning and scope of section 6(2)(b) of the Human Rights Act 1998. This, rather than the policy debate outlined above, is the important issue in this case. If it is resolved in favour of (i) or (ii) and against (iii), then the choice between (i) and (ii) depends upon what the court considers a "just and
D appropriate" remedy under section 8(1) of the 1998 Act. I should say at once that on both issues I agree with the conclusions reached by Lord Dyson JSC.

66 Under section 6(1) of the Act, it is unlawful for a public authority to act in a way which is incompatible with a Convention right. But the sovereignty of Parliament requires that exceptions be made for certain things which are done pursuant to an Act of the United Kingdom Parliament. As the annotations to the Act (by Peter Duffy QC and Paul Stanley) in
E *Current Law Statutes* explain, the exceptions

> "are all designed to prevent section 6 being used to circumvent the general principle of the Act embodied in sections 3(2)(b) and 4(6)(a), that incompatible primary legislation shall remain fully effective unless and until repealed or modified."

F In that event, the most that the court can do is make a declaration under section 4(2) that the Act is incompatible and leave it to Parliament to decide what, if anything, to do about it. It follows, however, that the exceptions must be read along with section 3(1). Section 3(1) requires that "So far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights". This obligation is laid upon everyone, not just upon the courts.

G 67 Two exceptions to the general rule in section 6(1) are provided by section 6(2). Section 6(2)(a) has presented little difficulty: it provides that subsection (1) does not apply if "as the result of one or more provisions of primary legislation, the authority could not have acted differently". This covers situations where the public authority was required by an incompatible Act of Parliament to do as it did (or perhaps where it had a
H choice between various courses of action, each of which was incompatible with the Convention rights). Although section 6(2)(a) does not say so, it must be read subject to section 3(1). So both the public authority and the courts, in deciding whether or not the authority could have acted differently, will have first to decide whether the Act of Parliament can be read or given effect in a way which is compatible rather than incompatible with the

Convention rights. If the Act can be read compatibly, then it follows that the authority could have acted differently and will have no defence if it has acted incompatibly.

68 Section 6(2)(b) makes the link with section 3(1) explicit, but has caused much more difficulty in practice. It provides that section 6(1) does not apply to an act (or failure to act) if

> "in the case of one or more provisions of, or made under, primary legislation which cannot be read or given effect in a way which is compatible with the Convention rights, the authority was acting so as to give effect to or enforce those provisions."

So the first question is always whether the primary legislation can be read or given effect in a compatible way. If it can, that is an end of the matter: see *Manchester City Council v Pinnock (Secretary of State for Communities and Local Government intervening)* [2010] 3 WLR 1441, paras 93–103. In that case, both the provision requiring the court to make a possession order in respect of a demoted tenancy and the provision empowering the local authority to seek one could be read and given effect in a compatible way. This bears out the prediction by Beatson and others, in *Human Rights: Judicial Protection in the United Kingdom* (2008), para 6-23, that cases where legislation cannot be read down under section 3 "are likely to be rare". However, if the legislation cannot be so read *or* given effect, the second question is whether the public authority was acting so as to give effect to or enforce it. As to this, it is possible to detect some differences of opinion among the judges. Some have taken the view that the fact that there may be choices involved in whether or not to give effect to or enforce the incompatible provision makes no difference: the authority was acting so as to give effect to or enforce it. Others, most notably Lord Mance in the *Doherty* case [2009] AC 367, would draw a distinction between the court, which might have no choice but to give effect to an incompatible provision, and the public authority bringing the proceedings, which could choose whether or not to do so and should be guided by Convention values when making its decisions.

69 Fortunately, we do not have to resolve that debate. This case is about the first question: can section 64(1A) be read and given effect compatibly with the Convention rights? In my view it clearly can. This is for two principal reasons. The first relates to the requirement to "read"—that is, interpret—statutory language compatibly with the Convention rights. In this case, to say that section 64(1A) cannot be so read involves reading "may be retained" as "must be retained, save in exceptional circumstances". This would be doing the reverse of what section 3(1) requires. In other words, it would be reading into words which *can* be read compatibly with the Convention rights a meaning which is incompatible with those rights. It would be giving the broad discretion provided in section 64(1A) an unnatural or strained meaning to require it to be given effect in an incompatible way.

70 That view is reinforced by the fact that it was the clear intention of Parliament to legislate compatibly rather than incompatibly with the Convention rights. Section 64(1A) was introduced into PACE by section 82 of the Criminal Justice and Police Act 2001. When the Bill which became that Act was introduced into Parliament, it was prefaced by the ministerial statement required by section 19(1)(a) of the Human Rights Act 1998.

A The Home Secretary, Mr Straw, stated that "In my view the provisions of the Criminal Justice and Police Bill are compatible with the Convention rights". He was not alone in that view. After all, the House of Lords in *Marper UK* [2004] 1 WLR 2196 unanimously took the view that section 64(1A) was compatible with the Convention rights. But this does not suggest to me that Parliament's intention was that the apparent discretion which it conferred
B should inevitably be read incompatibly with the Convention rights should that view later prove to be unfounded. Quite the reverse.

71 The second relates to the requirement in section 3(1) that legislation be "given effect" compatibly with the Convention rights. As Lord Rodger of Earlsferry emphasised in *Ghaidan v Godin-Mendoza* [2004] 2 AC 557, para 107, section 3(1) contains not one, but two, obligations. In retrospect, that is what the Court of Appeal had in mind in the case which became
C *In re S (Minors) (Care Order: Implementation of Care Plan)* [2002] 2 AC 291: that the court's power to make a care order giving the local authority enhanced (that is, determinative) parental responsibility for a child should be given effect in such a way as to prevent the local authority exercising that responsibility incompatibly with the Convention rights of either the child or his parents. Also in retrospect, one can see that the proper remedy for
D incompatible actions by the local authority is a freestanding action under section 7(1)(a) of the Human Rights Act 1998, rather than by the care court adopting powers which contradicted the "cardinal principle" of the separation of powers between court and local authority in care proceedings.

72 *In re S* is the strongest case in favour of the position adopted by the commissioner and the Secretary of State in this case. They have to argue that, despite ostensibly giving the police a discretion, the "cardinal
E principle" was, not that data may be kept, but that they must be kept. The ACPO guidelines could say only one thing. Further, they must argue that that principle is so fundamental to the legislative purpose that only Parliament can modify it if it turns out that those guidelines are incompatible with the Convention rights. I can readily accept that it may be desirable for Parliament rather than ACPO to put something in its place. But I cannot see
F how it was possible for the discretion conferred by section 64(1A) to be exercised in accordance with ACPO guidelines when it was first enacted but it is not possible for it to be so exercised now. In other words, if it was possible to read and give effect to section 64(1A) by means of ACPO guidelines when it was first enacted, it must be possible to do so now. And ACPO as a public authority has to act compatibly with the Convention rights. For these reasons, therefore, section 64(1A) is not incompatible with
G the Convention rights and cannot be so declared.

73 However, the need for a consistent national approach must be relevant to the choice between remedy (i) and remedy (ii). The court is empowered by section 8(1) to grant such relief or remedy in relation to an unlawful act "as it considers just and appropriate". There would be nothing to stop ACPO promulgating some new and Convention-compliant
H guidelines. Now that *Marper UK* [2004] 1 WLR 2196 has been overruled, they clearly should set about doing so unless Parliament does it for them within a reasonably short time. But I certainly accept that the system will not work if different police forces adopt different policies. So it would not be "appropriate" (such a flexible word) for this court to make mandatory decisions in individual cases unless and until it becomes clear that neither

237

ACPO nor Parliament is prepared to make the difficult choices involved. I therefore agree that we should declare the current guidelines unlawful but grant no further relief.

LORD JUDGE CJ

74 I agree with the reasoning and conclusions of the majority of the members of the court. In deference to the contrary views I shall add some brief words of my own.

75 The insertion of section 64(1A) in the Police and Criminal Evidence Act 1984 by section 82 of the Criminal Justice and Police Act 2001 resulted in the promulgation of the *Retention Guidelines for Nominal Records on the Police National Computer* (the ACPO guidelines) 2006. Thereafter in England and Wales the retention of biometric data (DNA samples) was governed by these guidelines which derived their authority from section 64(1A).

76 The judicial examination of these provisions in England and Wales culminated in a decision of the House of Lords in *R (S) v Chief Constable of the South Yorkshire Police; R (Marper) v Chief Constable of the South Yorkshire Police* [2004] 1 WLR 2196 that the retention of DNA samples did not constitute an interference with the rights granted by article 8 of the European Convention of Human Rights, or if it did, that the interference was modest and proportionate.

77 The Grand Chamber of the European Court of Human Rights disagreed, and concluded that the system created by the ACPO guidelines constituted an interference with article 8 rights: *S v United Kingdom* 48 EHRR 1169. Taking account of the decision and applying its reasoning we are all agreed that the decision of the House of Lords should no longer be treated as authoritative. Therefore these appeals must be allowed.

78 The forensic battle is directed at the consequences which should now flow.

79 The starting point is the reasoning of the Grand Chamber which identified the way in which different member states addressed the retention issue, and acknowledged that even following acquittal, it was permissible, subject to specific limitations within the domestic arrangements, for DNA samples to be retained. What however was required of any arrangements for retention was an approach which discriminated "between different kinds of cases and for the application of strictly defined storage periods for data, even in more serious cases". Attention was drawn to the position in Scotland where the legislative arrangements permitted the retention of the DNA of unconvicted individuals, limited in the case of adults to those "charged with violent or sexual offences and even then, for three years only", with the possibility of an extension for a further two years with judicial agreement. These arrangements were not criticised. Indeed the court acknowledged that the retention of DNA profiles represented the legitimate purpose "of assisting in the identification of future offenders". In short the existence of the legislative provisions for the retention of DNA samples was endorsed, but criticism was directed at the "blanket and indiscriminate nature of the power of retention" found in the ACPO guidelines.

80 Accordingly nothing in the judgment of the court leads to the conclusion that a different, less all encompassing scheme deriving its authority from section 64(1A) would contravene article 8, or that the law in

A relation to DNA samples should revert to the former wide-ranging prohibition against the retention of samples of any kind which was the striking feature of section 64 of the 1984 Act as originally enacted. Rather the judgement confirmed that legislative arrangements may provide for the retention of the DNA samples of those acquitted of criminal offences. That is what section 64(1A), reversing the provisions of section 64, permits.

B 81 In these circumstances it was open to ACPO to reconsider and amend the guidelines (as indeed, at least in part, it did) in the light of the decision of the European court, and it would be open to ACPO to do so in the light of the decision of this court. Section 64(1A) does not preclude an amendment to the guidelines which addresses the criticisms. In other words, although the process of further amendment to the arrangements for the retention of DNA samples in England and Wales has been and continues to be addressed C through legislation, this was not and is not the only way to provide for the protection of article 8 rights against the current scheme for their indiscriminate retention. In my judgment section 64(1A) is Convention compliant, whereas the ACPO guidelines in their present form are not. Accordingly, the retention of the DNA samples of these claimants was unlawful, but a declaration of incompatibility would be inappropriate.

D LORD KERR OF TONAGHMORE JSC

82 Lord Rodger of Earlsferry and Lord Brown of Eaton-under-Heywood JJSC in powerfully reasoned judgments, which I initially found persuasive, have concluded that section 64(1A) of the Police and Criminal Evidence Act 1984 (PACE) had as its purpose the institution of a scheme for the indefinite retention of biometric data taken from all suspects (with very E limited exceptions) in connection with the investigation of offences. On that account they found that, despite the seemingly permissive language of the subsection, the Association of Chief Police Officers (ACPO), to whom the task of drawing up guidelines for the implementation of section 64(1A) had been entrusted, were obliged to ensure that, instead of being destroyed as previously required by section 64(1) of PACE, samples taken from suspects F would be retained indefinitely and so remain available to the police on the national DNA database.

83 If indefinite retention of data was indeed section 64(1A)'s unmistakable purpose, I would have readily agreed that the discretion that "samples *may* be retained after they have fulfilled the purposes for which they were taken" would have to be exercised so as to give effect to that intention. That, as Lord Rodger JSC has said, would be the inevitable G consequence of the application of the principle for which *Padfield v Minister of Agriculture, Fisheries and Food* [1968] AC 997 is the seminal authority: that a discretion conferred with the intention that it should be used to promote the policy and objects of the Act can only be validly exercised in a manner that will advance that policy and those objects. More pertinently, the discretion may not be exercised in a way that would frustrate the H legislation's objectives. Everything therefore depends on what one decides is the true intention or purpose of the legislation.

84 This is not as easy a question to answer as the simple formulation, "what was the purpose of the legislation", suggests. As Lord Brown JSC has pointed out in para 145 of his judgment, the search for the purpose of a particular item of legislation may have to follow a number of avenues and

239

may require consideration of several aspects of the enactment—what is the grain of the legislation, what its underlying thrust etc. An important factor in the conclusion on this critical question which Lord Rodger JSC has identified is the fact that Parliament clearly saw the need for retreat from the position that had hitherto obtained under section 64(1)(3) of PACE as originally enacted. Those subsections were in these terms:

"(1) If— (a) fingerprints or samples are taken from a person in connection with the investigation of an offence; and (b) he is cleared of that offence, they must be destroyed as soon as is practicable after the conclusion of the proceedings."

"(3) If— (a) fingerprints or samples are taken from a person in connection with the investigation of an offence; and (b) that person is not suspected of having committed the offence, they must be destroyed as soon as they have fulfilled the purpose for which they were taken."

85 As Lord Rodger JSC has pointed out, the decision of the House of Lords in *Attorney General's Reference (No 3 of 1999)* [2001] 2 AC 91 brought to the attention of the public and Parliament the effect of these provisions. Potentially useful evidence was not being used for reasons that, as Lord Steyn put it, were "contrary to good sense": see p 118. No doubt reaction to the experience in that case contributed to Parliament's decision to enact section 64(1A) but did it, as Lord Rodger JSC has concluded, lead to Parliament's resolve that samples taken from suspects would be retained indefinitely and so remain available to the police on the national DNA database? In my judgment, and largely for the reasons given by Lord Dyson JSC, it did not.

86 In the first place, if that was Parliament's intention it chose a curious way to achieve it. A simple, unambiguous provision to that effect would not have been difficult to devise. And if the purpose of the legislation was to obtain a blanket, universally applied (apart from exceptional cases) policy, why would Parliament have left the practicalities of implementing the policy to ACPO? The drafting of the provision at a level of generality surely suggests that Parliament intended a measure of flexibility to be a feature of its application. This is unsurprising. The history of evolving knowledge as to the use to which DNA evidence could be put provided the clearest possible reasons not to adopt over prescriptive rules that might impede its full exploitation in circumstances unforeseen at the time of their enactment. Just as it was judged, in retrospect, to be unwise to have an immutable requirement to destroy all samples from certain categories of suspects and defendants, so also it would be unwise to substitute that obligation with a blanket requirement to retain all samples.

87 Various members of the Appellate Committee of the House of Lords in *R (S) v Chief Constable of the South Yorkshire Police; R (Marper) v Chief Constable of the South Yorkshire Police* [2004] 1 WLR 2196 described the benefits that can flow from the maintenance of an expanded database for DNA samples and I am in respectful agreement with all that Lord Steyn, Baroness Hale of Richmond and Lord Brown of Eaton-under-Heywood had to say on this subject in that case. But I do not consider that it necessarily follows that an inflexible policy requiring retention of virtually every sample taken from suspects and defendants is needed in order to have a viable and worthwhile resource.

88 Whatever view one takes of the competing policy arguments on this issue, however, it is, to my mind, quite clear that Parliament did not intend that this was the only way in which the legislation could be implemented. Not only does section 64(1A) use the permissive "may" in relation to the retention of samples but subsection (3) is retained in its original state, albeit that it may now be disapplied in a variety of circumstances outlined in section 64(3AA) to (3AD) (as inserted by section 82(4) of the Criminal Justice and Police Act 2001). This seems to me clearly to indicate recognition that there should be limits on the retention of samples but, not surprisingly, Parliament did not attempt to forecast comprehensively what those limits should be. The structure of the new section 64 is strongly suggestive of an intention to devise a scheme that would respond to developments in this field, not least any view that might be taken as to the human rights implications that might come to be recognised. As Lord Dyson JSC has put it, Parliament's intention must be taken to have been to create a proportionate scheme which is compatible with the Convention. There is nothing to impel the conclusion that Parliament intended that the scheme could not adapt to whatever the compatibility requirements were found to be. On the contrary, there is every reason to suppose that Parliament intended that the scheme could be adapted to meet those requirements as and when they became apparent.

89 What the commissioner and the Secretary of State's argument resolves to is that, in interpreting section 64, we should recognise that an underlying, not expressly articulated, purpose was that the samples *had to be* retained indefinitely, regardless of the circumstances in which they were taken or of the circumstances of the individual from whom they had been taken. There is nothing in the language of the section itself that compels such an exclusive interpretation. Indeed, as Lord Phillips of Worth Matravers PSC has pointed out, acceptance of this argument would involve reading more into section 64(1A) than its ordinary language conveys.

90 ACPO's guidelines were an essential complement to the statutory scheme. Those guidelines have been altered (in relation to children under 10) as a result of the decision of the Grand Chamber in *S and Marper v United Kingdom* 48 EHRR 1169. There is no lawful impediment to ACPO devising and implementing guidelines that take full account of the other features which the Grand Chamber has decreed are necessary for the operation of the scheme to be Convention compliant. Classifications (as to which categories of offences or individuals should require retention of samples) and long stop provisions (as to the period that they should be retained) are well within the institutional reach of ACPO. So also are the circumstances in which exceptions to the guidelines can be permitted. ACPO chose the exceptionality criteria. They may equally change those criteria. And because there is no legal impediment in them doing so, then under section 6 of HRA, they or Parliament must. Section 6(2)(b) can only come into play if ACPO cannot act. If it can, then it must.

91 Because parliamentary change is imminent, however, and because significant policy issues need to be considered, it is not unreasonable to leave this to Parliament. I therefore agree with the order proposed by Lord Dyson JSC.

92 I also agree with all that Lord Dyson JSC has had to say on the argument that Parliament could not have intended to entrust the creation of a detailed scheme pursuant to section 64(1A) to the police subject only to the

241

judicial review jurisdiction of the court. As he has said, the scope of the argument is confined. It is to the effect that, although it could have done so if it had considered it appropriate, Parliament must be taken not to have intended to grant such a power because of the constitutional and institutional limits on the competence of the police. But Parliament does not appear to have felt such qualms in giving the initial responsibility for the devising of guidelines to ACPO and, as Lord Dyson JSC has pointed out, no question of constitutional competence arises.

93 Finally, I agree with Lord Dyson JSC's conclusion on the discrete issue of GC's photographs.

Dissenting judgments on the appropriate relief

LORD RODGER OF EARLSFERRY JSC

94 In September 1984 Sir Alec Jeffreys made his ground-breaking discovery of DNA "fingerprints". A few weeks later, on 31 October, the Police and Criminal Evidence Act 1984 ("PACE") was enacted. Within a few years Sir Alec's discovery was being used routinely in the criminal courts in this country. Section 64(1) of PACE, as originally enacted in ignorance of this major development that lay just ahead, provided:

> "If— (a) fingerprints or samples are taken from a person in connection with the investigation of an offence; and (b) he is cleared of that offence, they must be destroyed as soon as is practicable after the conclusion of the proceedings."

95 In January 1997 an unidentified intruder raped and assaulted a woman in her home in London. Swabs were taken from her and were found to contain semen. A DNA profile was obtained from the semen and placed on the national DNA database. In January 1998 a man was arrested for an unrelated offence of burglary. A saliva sample was taken from him and a DNA profile was derived from it. In August of the same year the man was acquitted of the burglary and, by virtue of section 64(1) of PACE, his sample should have been destroyed. In fact, however, his profile was left on the DNA database and in October a match was made between this profile and the DNA profile derived from the semen in the swabs taken from the woman who had been raped in January 1997. The man was arrested and a DNA profile was obtained from a hair plucked from him. As was to be expected, this profile also matched the DNA derived from the semen. At his trial for the rape the judge held, however, that, since the material which had led to his identification should have been destroyed as required by section 64(1), the evidence relating to the profile from the plucked hair was not admissible. The man was acquitted. The Attorney General referred the matter to the Court of Appeal who agreed with the judge but referred the point to the House of Lords. In *Attorney General's Reference (No 3 of 1999)* [2001] 2 AC 91 the House reversed the Court of Appeal. The speech of Lord Steyn, with which the other members of the Appellate Committee agreed, was notable for his observation, at p 118, that the "austere" interpretation of the Court of Appeal produced results which were "contrary to good sense".

96 For present purposes, that case is important because it alerted the public and politicians to the fact that the obligation under section 64(1) of PACE to destroy samples if the suspect was acquitted meant that evidence

A which might lead to the detection and prosecution of the perpetrators of other crimes would be lost. Just a few weeks after their Lordships' decision, in the course of the second reading debate on the Criminal Justice and Police Bill, the Home Secretary introduced Part IV of the Bill which, he explained, was designed, inter alia, to amend section 64(1) of PACE to prevent evidence being lost in this way. The Home Secretary referred to Lord Steyn's speech
B as demonstrating the need for the change: Hansard (HC Debates), 29 January 2001, col 42.

97 This history shows beyond doubt that Parliament's purpose in enacting section 82 of the Criminal Justice and Police Act 2001, which inserted section 64(1A) into PACE, was to ensure that, in future, instead of being destroyed, samples taken from suspects would be retained indefinitely and so remain available to the police on the national DNA database.
C This would protect the public by facilitating the detection and prosecution of the perpetrators of crimes. Section 64(1A) (as inserted by section 82 of the Criminal Justice and Police Act 2001 and amended by sections 117(7) and 118(4)(a) of the Serious Organised Crime and Police Act 2005) provides:

> "Where— (a) fingerprints, impressions of footwear or samples are taken from a person in connection with the investigation of an offence,
D and (b) subsection (3) below does not require them to be destroyed, the fingerprints, impressions of footwear or samples may be retained after they have fulfilled the purposes for which they were taken but shall not be used by any person except for purposes related to the prevention or detection of crime, the investigation of an offence, the conduct of a prosecution or the identification of a deceased person or of the person
E from whom a body part came."

98 After this provision came into force, in accordance with guidelines from the Association of Chief Police Officers ("ACPO") the police proceeded to retain data indefinitely and so to build up their DNA database of samples and profiles obtained from people who had been suspected of crimes, even if they had not been prosecuted or had been acquitted.

F 99 In due course in two appeals to the House of Lords this system was challenged as being in violation of the suspects' article 8 Convention rights: *R (S) v Chief Constable of the South Yorkshire Police; R (Marper) v Chief Constable of the South Yorkshire Police* [2004] 1 WLR 2196. In the leading speech Lord Steyn said, at para 2, that "as a matter of policy it is a high priority that police forces should expand the use of [DNA] evidence where possible and practicable". He went on to refer to public disquiet that the
G obligation to destroy samples under the unamended section 64(1) of PACE had sometimes enabled defendants who had in all likelihood committed grave crimes to walk free. Baroness Hale of Richmond observed, at para 78, that

> "The present system is designed to allow the collection of as many samples as possible and to retain as much as possible of what it has.
H The benefit to the aims of accurate and efficient law enforcement is thereby enhanced."

100 In the light of such considerations the House of Lords held unanimously that the system did not violate the applicants' article 8 Convention rights.

243

101 To the European Court of Human Rights, however, the matter appeared differently. In *S v United Kingdom* 48 EHRR 1169 the Grand Chamber first held unanimously—and contrary to the majority view in the House of Lords—that the English system did indeed involve an interference with suspects' article 8 rights. Then, when considering the proportionality of that interference, the court observed, at para 119:

> "In this respect, the court is struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken—and retained—from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the nationwide database or the materials destroyed; in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances."

The court went on to conclude, at para 125:

> "that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent state has overstepped any acceptable margin of appreciation in this regard. Accordingly, the retention at issue constitutes a disproportionate interference with the applicants' right to respect for private life and cannot be regarded as necessary in a democratic society."

102 In response to the European court's judgment the last Parliament passed the Crime and Security Act 2010, section 14 of which was designed to amend section 64 of PACE with a view to establishing a regime for the retention and destruction of DNA material and profiles that would be compatible with article 8 as interpreted by the European court. The new Government, which came into office in May 2010, decided, however, not to commence this legislation. Instead, in Chapter 1 of Part 1 of the Protection of Freedoms Bill, it has put fresh legislative proposals, along similar lines to the legislation in Scotland, before Parliament. There were indications in the European court's judgment that a system along those lines would indeed be compatible with article 8. As in the earlier legislation, the complex proposals include provision for a National DNA Database Strategy Board to oversee the operation of the DNA database.

103 Obviously, in the light of the European court's judgment the indefinite retention of the data relating to the claimants under the existing system is incompatible with their article 8 rights. The decision of the House of Lords to the contrary in *R (S) v Chief Constable of the South Yorkshire Police; R (Marper) v Chief Constable of the South Yorkshire Police*

A [2004] 1 WLR 2196 must accordingly be overruled. That is accepted by the respondent, the Commissioner of Police of the Metropolis, and by the Home Secretary, who has intervened in the proceedings. Where the commissioner and the Home Secretary part company with the claimants is as to the order, if any, which the court should pronounce in these circumstances.

104 In effect, for the claimant C Mr Fordham argued that section 64(1A) is worded ("may be retained") so as to give the commissioner and chief B constables an open discretion as to whether data should be retained and, if so, for how long and subject to what conditions. The position was therefore quite straightforward. By virtue of section 6(1) of the Human Rights Act 1998 the commissioner and chief constables were obliged to exercise that discretion so as to establish and maintain a system for the retention of samples and data that would comply with suspects' article 8 Convention C rights as they are now to be interpreted in the light of the decision of the European court. It was unlawful for them not to do so. Mr Fordham indicated that he would be content for the court to pronounce a declaration to this effect, without making any order for the removal of the data relating to his client. While adopting the bulk of Mr Fordham's submissions, on behalf of the claimant GC, Mr Cragg asked the court to go further and indicate that in his case the position should be put right within 28 days. D

105 Mr Fordham's argument is, of course, unanswerable if he is right to say that the crucial words ("may be retained") in section 64(1A) confer a wide—indeed open—discretion on the commissioner and the chief constables whose forces retain the samples and data that make up the national DNA database. If that is correct, then, even though, when section 64(1A) came into force, ACPO issued guidelines requiring that— E subject to a narrow exception—all the DNA samples and data relating to suspects should be retained indefinitely, the association could with equal propriety have issued completely different guidelines which would have resulted in a system that did not provide for the indefinite retention of the samples and data. On that interpretation, any credit for the creation of the present DNA database is to be accorded to ACPO for choosing, of its own F freewill, to issue the guidelines which it did. More particularly, since ACPO had been, and still was, free to adopt other completely different guidelines, ACPO could now issue fresh guidelines which would produce a system that was compatible with the European court's judgment.

106 The key question, therefore, is whether Mr Fordham's construction of section 64(1A) as conferring this wide discretion on the police is correct. On behalf of the commissioner Lord Pannick argued that it is not. He drew G attention to the context, which I have already described, in which Parliament enacted section 64(1A). This showed that Parliament had set out to cure the mischief that the original version of section 64(1) of PACE meant that suspects' samples and data were removed from the database even although—as *Attorney General's Reference (No 3 of 1999)* [2001] 2 AC 91 demonstrated—the retention of that material could potentially result in the detection and prosecution of serious criminals. Parliament plainly H intended that in future this material should be retained on the DNA database indefinitely. In other words, under section 64(1A) the police had to retain it indefinitely. Mr Fordham said, rhetorically, that, if this were correct, then the Home Secretary could have brought proceedings against the police if they had failed to retain the material indefinitely. Accepting the challenge,

Mr Eadie said that, while the matter would probably have been sorted out in a different way, if necessary, such proceedings could indeed have been brought.

107 It is useful to notice just how far reaching Mr Fordham's argument is: essentially, under section 64(1A) the police were free to do what they liked. On his approach the provision contained nothing to delimit the exercise of their discretion. When listening to his argument, at times I felt that—unconsciously, of course—he was intent on pulling down one of the most important bulwarks which our predecessors so painstakingly erected against arbitrary acts of the executive. In *Car Owners' Mutual Insurance Co Ltd v Treasurer of the Commonwealth of Australia* [1970] AC 527, 537E–F, Lord Wilberforce observed that "in a statutory framework it is impossible to conceive of a discretion not controlled by any standard or consideration stated, or to be elicited from, the terms of the Act". He was, of course, reflecting the thinking in *Padfield v Minister of Agriculture, Fisheries and Food* [1968] AC 997, 1030B–D, where Lord Reid had said that

> "Parliament must have conferred the discretion with the intention that it should be used to promote the policy and objects of the Act; the policy and objects of the Act must be determined by construing the Act as a whole and construction is always a matter of law for the court."

108 Following that classic authority, in my view the power which was conferred on the police by section 64(1A) had to be exercised in accord with the policy and objects of that enactment. As I have explained, the policy and objects of Parliament in enacting section 64(1A) were plainly that DNA samples and data derived from suspects should be retained indefinitely so that a large and expanding database should be available to aid the detection and prosecution of the perpetrators of crimes. The police were therefore bound to exercise the power given to them by section 64(1A) in order to promote that policy and those objects. This meant, in effect, that, subject to possible very narrow exceptions (e g, those suspected of a crime which turned out not to be a crime at all), the police had to retain on their database the samples and profiles of all suspects. In short, the police were under a duty to do so. By a slightly different route this analysis reaches the same result as the older well known line of authority to the effect that, on the proper construction of a statute as a whole and in its context, it can sometimes be seen that a power granted to, say, an official, court or other body in the public interest must be regarded as having been coupled with an implied duty on the recipient to exercise the power in the circumstances envisaged for its exercise. See, for instance, *Julius v Bishop of Oxford* (1880) 5 App Cas 214; *Attorney General v Antigua Times Ltd* [1976] AC 16, 33F–G, per Lord Fraser of Tullybelton.

109 In my view, therefore, given the policy and objects of the enactment, before the decision of the European court the police could not have exercised their power under section 64(1A) by choosing to retain samples and data for, say, only three years (or any other period deliberately not prescribed in the legislation) and then destroying them. Similarly, given the policy and objects of the enactment, the police could not have exercised the power to detain material indefinitely by choosing to delete material from those against whom, in their view, suspicion fell below some arbitrary level not recognised in the legislation. Any such exercise of their power would

have defeated, rather than promoted, the policy of the enactment and would therefore have been unlawful.

110 In the light of the European court's decision, it can now be seen that the policy and objects of section 64(1A), to create a virtually comprehensive and expanding database of DNA profiles from suspects, violate the article 8 Convention rights of unconvicted suspects. Given that the Protection of Freedoms Bill has been introduced into Parliament, there is good reason to believe that legislation will be passed in the foreseeable future to establish a new system. The question in the present proceedings is whether in the meantime, by virtue of section 3(1) of the HRA or otherwise, the police must read and give effect to section 64(1A) in a way that is compatible with article 8 as interpreted by the European court—and whether they act unlawfully if they do not.

111 Since I reject Mr Fordham's argument that section 64(1A) gives the police an open discretion as to what to do, I also reject his further, seductive, argument that, having regard to section 6(1) of the HRA, they can and should simply exercise that discretion in such a way as to establish a lawful system that meets the requirements of the European Court of Human Rights—for example, by choosing to retain samples and data for only three years, subject, perhaps, to a power in an independent body to extend the period for some further defined period (as under the Scottish legislation), or by only retaining the material from those suspected of certain classes of crimes, or by only retaining the material from those against whom there is a high degree of suspicion etc.

112 All of those suggested steps would have been inconsistent with the policy and objects of section 64(1A) as originally enacted. So they could only be adopted now, in order to comply with the European court's decision, if section 3(1) of the HRA makes that not only possible but indeed obligatory.

113 Section 3 provides:

> "(1) So far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights.
>
> "(2) This section— (a) applies to primary legislation and subordinate legislation whenever enacted; (b) does not affect the validity, continuing operation or enforcement of any incompatible primary legislation; and (c) does not affect the validity, continuing operation or enforcement of any incompatible subordinate legislation if (disregarding any possibility of revocation) primary legislation prevents removal of the incompatibility."

The opening phrase in subsection (1) shows that there are limits to the duty which it imposes. The words of Lord Nicholls of Birkenhead in *In re S (Minors) (Care Order: Implementation of Care Plan)* [2002] 2 AC 291, para 40, are a useful guide to where those limits lie:

> "For present purposes it is sufficient to say that a meaning which departs substantially from a fundamental feature of an Act of Parliament is likely to have crossed the boundary between interpretation and amendment. This is especially so where the departure has important practical repercussions which the court is not equipped to evaluate. In such a case the overall contextual setting may leave no scope for

247

rendering the statutory provision Convention compliant by legitimate use of the process of interpretation." A

114 Mr Fordham submitted that the fundamental feature of section 64(1A) was the retention of the material for the purposes of creating a DNA database, not the indefinite retention of the material with a view to establishing a virtually comprehensive database of DNA material from suspects. In my view that submission is unrealistic. The truth is that B Parliament wanted to eliminate the danger, which existed under the pre-existing legislation, that valuable evidence would be lost and potential prosecutions of the guilty based on the latest science would be jeopardised if material had to be removed from the database. Providing for the material to be retained on the database indefinitely was therefore *the* fundamental feature of the amending legislation which inserted section 64(1A) into PACE. C

115 That being so, section 3(1) of the HRA does not oblige or permit the courts or the police to read or give effect to section 64(1A) in a way that departs substantially from that fundamental feature. And it is quite obvious that any reading of section 64(1A) which would be apt to obviate the defects identified in the existing system by the European court would depart very substantially indeed from that fundamental feature of the provision— D would, indeed, contradict it. It is therefore nothing to the point that, from a linguistic point of view, the provision might easily be read as though it said that samples "may be retained, *consistently with the suspects' article 8 Convention rights* . . ." The hypothetical additional words, though few in number, would have the effect, and would be intended to have the effect, of altering the provision so as, say, to limit the samples and data that were to be retained and the time for which they could be retained, and to impose a duty E to remove them after that time—and so to negate the defining feature of the legislation. In other words, the court would have crossed the line from interpreting to amending the legislation. Amending section 64(1A) in that way is something which only Parliament can do. Parliament showed itself willing to pass amending legislation in the Crime and Security Act 2010. The fact that the new Government decided not to commence that legislation, F but chose to introduce a Bill providing for a different scheme shows that there is a range of possible ways to bring the system into line with the requirements of article 8 and room for doubt about which is the best policy to adopt. This court is in no position to weigh the competing practical advantages and disadvantages of the possible solutions. These are further features which confirm that the necessary changes require legislation and G cannot be made by any legitimate interpretation, however extensive, under section 3(1): *In re S (Minors) (Care Order: Implementation of Care Plan)* [2002] 2 AC 291, para 40, per Lord Nicholls.

116 Section 64(1A) is therefore incompatible with suspects' article 8 Convention rights and cannot be made compatible under section 3(1) of the HRA. Section 3(2)(b) ensures that in these circumstances the continuing operation of section 64(1A) is unaffected. Section 6(1)(2) provides: H

"(1) It is unlawful for a public authority to act in a way which is incompatible with a Convention right.

"(2) Subsection (1) does not apply to an act if— (a) as the result of one or more provisions of primary legislation, the authority could not have

A acted differently; or (b) in the case of one or more provisions of, or made under, primary legislation which cannot be read or given effect in a way which is compatible with the Convention rights, the authority was acting so as to give effect to or enforce those provisions."

Like sections 3(2) and 4(6), section 6(2) is concerned to preserve the primacy and legitimacy of primary legislation. See *Aston Cantlow and Wilmcote* B *with Billesley Parochial Church Council v Wallbank* [2004] 1 AC 546, para 19, per Lord Nicholls, cited with approval by Lord Hoffmann in *R (Hooper) v Secretary of State for Work and Pensions* [2005] 1 WLR 1681, para 51. If that is correct and section 3(1) of the HRA cannot be invoked in the present case, then section 64(1A) continues to operate, and Parliament intends it to operate, in the same way as when enacted. It therefore falls to C be interpreted and applied just as when enacted.

117 It is accepted that section 6(2)(a) applies to cases where the legislation, which cannot be read compatibly with Convention rights, imposed a duty on a public authority to act in one particular way—the authority "could not have acted differently". It follows, of course—as Lord Hoffmann remarked in the *Hooper* case, para 49—that, by contrast, section 6(2)(b)

D

> "assumes that the public authority could have acted differently but nevertheless excludes liability if it was giving effect to a statutory provision which cannot be read as Convention-compliant in accordance with section 3."

118 Since the Convention-non-compliant provision continues to E operate, any public authority which is exercising a power conferred by it must continue do so in a way that promotes the object and purposes for which the provision confers the power—and these are, ex hypothesi, incompatible with Convention rights. As Lord Hoffmann noted, section 6(2)(b) assumes, however, that under the relevant legislation the public authority could have acted in more than one way. For example, it might be that a public authority could have adopted either of two schemes, F A and B, both of which would have promoted the policy and objects of the legislation. So it cannot be said that, when it chose to adopt scheme A, the public authority could not have acted differently. Nevertheless, since, when it adopted scheme A, the authority was promoting the policy and objects of the primary legislation and so was acting to give effect to the legislation, section 6(2)(b) disapplies section 6(1) and ensures that the authority was G acting lawfully. In this way the primacy and legitimacy of the provision of primary legislation are preserved.

119 For all the reasons which I have set out, in the present case, in substance the police could really not have acted differently: in order to promote the object and purposes of section 64(1A) of PACE, they had to retain all the samples which they did, indefinitely. If that is so, then what the police did, and continue to do, falls within section 6(2)(a) and is accordingly H lawful.

120 Even if one assumes, however, that, while promoting the policy and objects of the legislation, the police could, for example, have recognised a slightly wider exception and so created a slightly different system, that does not matter. The same goes if, while promoting the policy and objects of the

249

legislation, the police could have chosen not to recognise even the very narrow exception which they did and could have decided to retain the samples and data relating to absolutely all suspects. In either event, even though the police could have done something (slightly) different, by doing what they actually did and are still doing, they were acting and are continuing to act so as to give effect to section 64(1A). Section 6(2)(b) of the HRA accordingly applies and so the police have at all times acted, and continue to act, lawfully.

121 In these circumstances section 64(1A) is incompatible with suspects' article 8 Convention rights. Even though Parliament and the Government have the matter under review, I consider that the better course is for this court to grant a declaration of incompatibility in terms of section 4(2) of the HRA. Cf *Bellinger v Bellinger (Lord Chancellor intervening)* [2003] 2 AC 467, para 55, per Lord Nicholls of Birkenhead. I would accordingly allow the appeals to the extent of making a declaration that section 64(1A) of the Police and Criminal Evidence Act 1984 is incompatible with the article 8 Convention rights of suspects.

LORD BROWN OF EATON-UNDER-HEYWOOD JSC

122 On 4 December 2008 the Grand Chamber of the European Court of Human Rights in *S v United Kingdom* 48 EHRR 1169 condemned on article 8 grounds the scheme for the indefinite retention of biometric data adopted in England and Wales pursuant to section 64(1A) of the Police and Criminal Evidence Act 1984 ("PACE"). The critical issue for decision on these appeals is whether, following that decision and pending the enactment by Government of a fresh legislative scheme compatible with article 8, the police have been acting unlawfully in continuing to operate the indefinite retention scheme. That in turn depends upon whether section 64(1A) can or "cannot be read or given effect in a way which is compatible with the Convention rights" within the meaning of section 6(2)(b) of the Human Rights Act 1998 ("the HRA").

123 Before turning to address this issue it is necessary to sketch out something of the background to the appeal and the circumstances in which the point now arises for decision.

124 These claimants are two amongst the 850,000 odd unconvicted persons whose profiles are kept on the national DNA database, their fingerprints and samples having been taken from them when they were arrested as suspects (from 2003, whether or not they were actually charged). This database has built up following Parliament's introduction on 11 May 2001 of section 64(1A) of PACE in substitution for the original section 64(1) which had required the destruction of a suspect's fingerprints and samples as soon as practicable after he was cleared. Section 64(1A) provides so far as is material:

> "Where . . . fingerprints, impressions of footwear or samples are taken from a person in connection with the investigation of an offence . . . [they] may be retained after they have fulfilled the purposes for which they were taken but shall not be used by any person except for purposes related to the prevention or detection of crime, the investigation of an offence, the conduct of a prosecution or the identification of a deceased person or of the person from whom a body part came."

125 In 2004 this change in the law was unsuccessfully challenged, principally on article 8 grounds, all the way up to the House of Lords, by two complainants: S, an 11-year-old boy with no previous convictions who had been acquitted of attempted robbery, and Mr Marper, a man of 38, also of good character, whose case was discontinued following his arrest on the charge of harassing his partner: *R (S) v Chief Constable of the South Yorkshire Police; R (Marper) v Chief Constable of the South Yorkshire Police* [2004] 1 WLR 2196. Baroness Hale of Richmond alone amongst the Appellate Committee thought that the retention and storage of DNA profiles constituted an interference with the applicants' rights under article 8. But each member of the Committee, Baroness Hale included, was quite clear that, even if it did, it was readily justifiable under article 8.2. Lord Steyn described such evidence as having "the inestimable value of cogency and objectivity" (para 1) and said that "as a matter of policy it is a high priority that police forces should expand the use of such evidence where possible and practicable": see para 2. At para 3 he observed that: "It can play a significant role in the elimination of the innocent, the correction of miscarriages of justice and the detection of the guilty." At paras 35–36 Lord Steyn dealt with a submission that retention is not "in accordance with law" (on the basis that "a law which confers a discretion must indicate the scope of that discretion": *Silver v United Kingdom* (1983) 5 EHRR 347, para 88):

> "The discretion involved in the power to retain fingerprints and samples makes allowance for exceptional circumstances, eg where an undertaking to destroy the fingerprints or sample was given or where they should not have been taken in the first place, as revealed by subsequent malicious prosecution proceedings."

At para 38 Lord Steyn observed that the "expansion of the database by the retention confers enormous advantages in the fight against serious crime" and at para 39 he remarked upon "the benefits of a greatly extended database". Lord Rodger of Earlsferry and Lord Carswell agreed with Lord Steyn. Baroness Hale agreed that retention and storage of DNA samples and profiles was "readily justifiable" for the reasons given by Lord Steyn and myself. She added:

> "The whole community, as well as the individuals whose samples are collected, benefits from there being as large a database as it is possible to have. The present system is designed to allow the collection of as many samples as possible and to retain as much as possible of what it has. The benefit to the aims of accurate and efficient law enforcement is thereby enhanced": para 78.

I myself suggested, at para 88,

> "that the benefits of the larger database . . . are so manifest . . . that the cause of human rights generally (including the better protection of society against the scourge of crime which dreadfully afflicts the lives of so many of its victims) would inevitably be better served by the database's expansion than by its proposed contraction. The more complete the database, the better the chance of detecting criminals, both those guilty of crimes past and those whose crimes are yet to be committed. The better

251

chance too of deterring from future crime those whose profiles are already on the database." A

And I pointed out too that: "The larger the database, the less call there will be to round up the usual suspects. Instead, those amongst the usual suspects who are innocent will at once be exonerated."

126 These views notwithstanding, the Grand Chamber in Strasbourg, 48 EHRR 1169, as already indicated, on the application of the same complainants, some four years later unanimously condemned the scheme as unjustifiable under article 8. It is sufficient for present purposes to quote just three paragraphs from the court's lengthy judgment: B

"119. . . . the court is struck by the blanket and indiscriminate nature of the power of retention in England and Wales. The material may be retained irrespective of the nature or gravity of the offence with which the individual was originally suspected or of the age of the suspected offender; fingerprints and samples may be taken—and retained—from a person of any age, arrested in connection with a recordable offence, which includes minor or non-imprisonable offences. The retention is not time limited; the material is retained indefinitely whatever the nature or seriousness of the offence of which the person was suspected. Moreover, there exist only limited possibilities for an acquitted individual to have the data removed from the nationwide database or the materials destroyed; in particular, there is no provision for independent review of the justification for the retention according to defined criteria, including such factors as the seriousness of the offence, previous arrests, the strength of the suspicion against the person and any other special circumstances." C D E

"125. In conclusion, the court finds that the blanket and indiscriminate nature of the powers of retention of the fingerprints, cellular samples and DNA profiles of persons suspected but not convicted of offences, as applied in the case of the present applicants, fails to strike a fair balance between the competing public and private interests and that the respondent state has overstepped any acceptable margin of appreciation in this regard . . ." F

"134 . . . In accordance with article 46 of the Convention, it will be for the respondent state to implement, under the supervision of the Committee of Ministers, appropriate general and/or individual measures to fulfil its obligations to secure the rights of the applicants and other persons in their position to respect for their private life." G

Before turning to the circumstances in which these particular claimants had their fingerprints and samples taken and the precise nature of the argument they advance on this appeal, it is convenient first to indicate something of the response to the Grand Chamber's judgment, on the part both of the Government and of the police.

127 So far as the Government was concerned, the then Home Secretary in a Press Release on 16 December 2008 indicated that the Home Office would institute a consultation process but that meantime: H

"The DNA of children under ten—the age of criminal responsibility—should no longer be held on the database. There are around 70 such cases

A [we are told that there were in fact 96], and we will take immediate steps to take them off."

(S and Mr Marper's data was also removed.)

128 On 7 May 2009 the Home Office published a White Paper, *Keeping the Right People on the DNA Database*, setting out certain key proposals for the future and inviting views upon them. The White Paper also considered B what should happen to the 850,000 odd profiles already on the national DNA database.

129 On 28 July 2009 ACPO's Director of Information wrote to all chief constables indicating that new guidelines were not expected to take effect until 2010 and that:

> "Until that time, the current retention policy on fingerprints and DNA C remains unchanged . . . ACPO strongly advise that decisions to remove records should not be based on proposed changes. It is therefore vitally important that any applications for removals of records should be considered against current legislation and 'the Retention Guidelines Exceptional Case Procedure . . ."

Those guidelines, which have remained essentially the same since D section 64(1A) was introduced, provide:

> "Chief Officers have the discretion to authorise the deletion of any specific data entry on the PNC 'owned' by them. They are also responsible for the authorisation of the destruction of DNA and fingerprints associated with that specific entry. It is suggested that this discretion should only be exercised in exceptional cases . . .
>
> E "Exceptional cases will by definition be rare. They might include cases where the original arrest or sampling was found to be unlawful. Additionally, where it is established beyond doubt that no offence existed, that might, having regard to all the circumstances, be viewed as an exceptional circumstance."

130 On 11 November 2009, following the consultation period, the F Home Secretary made a written ministerial statement outlining a revised set of proposals for the retention of fingerprints and DNA data: Hansard (HC Debates), 11 November 2009, col 25WS. It was originally intended to implement these by way of order-making powers under the Policing and Crime Act 2009 but, following strong opposition to the introduction of a new scheme by secondary rather than primary legislation, the proposed new G scheme was included in the Crime and Security Act 2010, introduced in the House of Commons on 19 November 2009 and receiving Royal Assent on 8 April 2010.

131 Following a change of government in May 2010, however, rather than bringing the Crime and Security Act into force, the incoming Government instead announced its proposal for new legislation designed essentially to mirror the Scottish system and this finally, by the Protection of H Freedoms Bill 2011, introduced in the House of Commons as recently as 11 February 2011, it has now set in train.

132 For reasons which will shortly become clear, it is unnecessary for the purposes of this judgment to indicate anything of the detailed nature of the various proposals which at one time or another have been considered for

enactment in substitution for the existing scheme so as to achieve compatibility with article 8 pursuant to the Grand Chamber judgment. It is sufficient to indicate that a wide range of differing schemes have been canvassed and considered and that arriving at the preferred solution has inevitably involved complex and sensitive choices.

133 It is similarly unnecessary to describe in any detail the facts of these claimants' cases and the following brief summary will suffice.

134 GC is 41. On 20 December 2007, following his girlfriend's complaint that he had assaulted her (albeit without causing her injury), he voluntarily attended the police station and was arrested on suspicion of common assault. He strongly denied the allegation, explaining rather that he had been defending himself against attack by her. Following the taking of DNA samples, fingerprints and a photograph, GC was released on police bail without charge. Before 21 February 2008, when he was due to surrender to his bail, GC was told that no further action would be taken against him. GC's fingerprints (but not DNA) had in fact been taken previously and retained in connection with a firearms offence for which he had been sentenced at the Central Criminal Court on 18 February 1992 to seven years' imprisonment.

135 C is 34, a man of good character. On 17 March 2009 he was arrested on suspicion of rape, harassment and fraud following allegations made the previous day by a former girlfriend and members of her family, allegations which C strenuously denied. The same day, C's fingerprints and DNA samples were taken. Although no further action was taken in relation to the alleged harassment and fraud, on 18 March 2009 C was charged with rape. On 5 May 2009, however, the prosecution offered no evidence on the rape charge and C was accordingly acquitted.

136 Both claimants, through solicitors, applied to the respondent police commissioner to have their fingerprints and DNA data deleted from police records—GC on 23 March 2009, C on 19 August 2009 (in each case, of course, after the Grand Chamber's decision in *S v United Kingdom* 48 EHRR 1169). Consistently with ACPO's guidelines, however, both applications were refused.

137 The claimants then issued judicial review proceedings, GC on 11 December 2009, C on 9 February 2010. The applications were heard together by the Divisional Court (Moses LJ and Wyn Williams J) on 15 July 2010 and on 16 July 2010 were dismissed, the Divisional Court correctly holding itself bound by the decision of the House of Lords in *R (S) v Chief Constable of the South Yorkshire Police; R (Marper) v Chief Constable of the South Yorkshire Police* [2004] 1 WLR 2196 (the subsequent Grand Chamber decision notwithstanding). The Divisional Court did, however, certify a point of law of general importance and, with the consent of all parties, granted a certificate pursuant to section 12 of the Administration of Justice Act 1969, thus enabling the matter to proceed directly to this court.

138 Before this court, Mr Fordham for C and Mr Cragg for GC both submit that, in the light of the Grand Chamber's judgment, the earlier decision of the House of Lords can no longer stand and the existing scheme must now be recognised to be unlawful—so much, indeed, is clear and conceded. Pursuant to section 6 of the HRA, their argument then continues, the police must now therefore cease retaining their data incompatibly with their article 8 rights. Instead, they submit, the police must take account of

254

A the various criticisms made by the Grand Chamber of the existing scheme, must devise a new, compatible scheme, and must then deal with these claimants' requests (and any other outstanding or future requests) for the removal of information from the national DNA database—this, indeed, in GC's case, within 28 days, contends Mr Cragg.

139 Not so, submit Lord Pannick for the Commissioner of Police of the
B Metropolis and Mr Eadie for the Home Secretary (properly joined in the proceedings as an interested party). It is, they submit, for the Government, not for the police, to devise and enact a new scheme; the police meantime have no alternative but to continue operating the existing scheme pursuant to section 64(1A) of PACE. Their case is founded on section 6(2)(b) of the HRA which, they argue, disapplies section 6(1) and thus relieves the police of liability for continuing to operate what the Grand Chamber has ruled to be
C (in international law) an unlawful scheme. The most the claimants are entitled to is a declaration of incompatibility pursuant to section 4 of the HRA.

140 As I indicated at the outset, this is the critical issue in the appeal and plainly it centres upon the proper understanding of, and interplay between, sections 3, 4 and 6 of the HRA which (as to their most material parts) I now
D set out:

> "3(1) So far as it is possible to do so, primary legislation and subordinate legislation must be read and given effect in a way which is compatible with the Convention rights."
>
> "4(2) If the court is satisfied that [a provision of primary legislation] is incompatible with a Convention right, it may make a declaration of that incompatibility."
>
> E "6(1) It is unlawful for a public authority to act in a way which is incompatible with a Convention right.
>
> "6(2) Subsection (1) does not apply to an act if— (a) as the result of one or more provisions of primary legislation, the authority could not have acted differently; or (b) in the case of one or more provisions of, or made under, primary legislation which cannot be read or given effect in a way
> F which is compatible with the Convention rights, the authority was acting so as to give effect to or enforce those provisions."

The precise symmetry between section 3(1) and section 6(2)(b) will at once be noted: each invites consideration of whether legislation can "be read or given effect in a way which is [Convention] compatible"—section 3 indicating what must be done if this is "possible", section 6(2)(b) indicating
G the consequence (the disapplication of section 6(1)) if it is not.

141 At first blush the commissioner's argument appears distinctly unpromising. Section 64(1A) is, after all, couched in terms that appear to confer on the police an open discretion: "samples may be retained." On the face of it, therefore, the police appear to be in a position to act compatibly with the article 8 rights of those whose samples have been taken and this, indeed, even without resort to section 3. But suppose there were some doubt
H about this, why would that not fall to be resolved by the interpretative imperative of section 3? How can it be appropriate, in the face of such a strong statutory direction, to place upon section 64(1A) a construction which denies the police the ability to exercise their data retention power compatibly? I confess to having come only comparatively late to the

conclusion that, difficult though the commissioner's argument initially appears, it is in fact correct.

142 Section 6(2)(b) has long been recognised to give rise to difficulty at the margins: see, for example, the judgments respectively of Lord Hope of Craighead, Lord Walker of Gestingthorpe and Lord Mance in *Doherty v Birmingham City Council* [2009] AC 367. Clearly, as Lord Hoffmann observed in *R (Hooper) v Secretary of State for Work and Pensions* [2005] 1 WLR 1681, para 49, section 6(2)(b)

> "assumes that the public authority could have acted differently but nevertheless excludes liability if it was giving effect to a statutory provision which cannot be read as Convention-compliant in accordance with section 3."

This, as was pointed out, was in contradistinction to section 6(2)(a) which applies when a public authority "could not have acted differently"—when, in other words, the authority has been compelled by primary legislation to act in a way ex hypothesi incompatible with Convention rights.

143 Superficially, of course, the very assumption that a public authority could have acted differently appears to postulate that the power in question could therefore have been exercised compatibly with Convention rights. Plainly, however, section 3 notwithstanding, it cannot follow that the power *must* therefore in all cases be exercised compatibly—else section 6(2)(b) could never come into play. A simple illustration of section 6(2)(b) in operation is, of course, where primary legislation confers a power on a public authority and where a decision to exercise that power (or, as the case may be, not to exercise it) would in every case inevitably give rise to an incompatibility. *R v Kansal (No 2)* [2002] 2 AC 69 was just such a case and in such situations it can readily be understood why section 6(2)(b) applies. Otherwise, instead of "giving effect to" a provision conferring a power, the public authority would have to treat the provision (in cases where not to exercise it would give rise to incompatibility) as if it imposed a duty—or, in cases where any exercise of the power would give rise to incompatibility (as in *R v Kansal (No 2)* itself), would have to abstain from ever exercising the power. In either instance, it is obvious, Parliament's will would be thwarted.

144 I would take this opportunity to resile from what I myself said in the latter part of para 118 of my own judgment in the *Hooper* case [2005] 1 WLR 1681. I was surely right to say in the first part of that paragraph:

> "Plainly it is not the case that section 6(2)(b) applies whenever a statutory discretion falls to be exercised in a particular way to ensure compliance with a Convention right. This occurs in a host of different situations and, so far as I am aware, no one has ever suggested that, had the discretion not been exercised compatibly, the public authority would nevertheless have been protected against a domestic law claim by the section 6(2)(b) defence on the basis that otherwise a power would be turned into a duty."

I was, however, wrong to suggest that the situation would be no different if to secure Convention compliance the statutory discretion had to be exercised in every case. It now seems to me that the underlying question in all these cases—indeed, the determinative question in every case lying between the two extremes I have thus far dealt with—is: what essentially was Parliament

256

intent on achieving by this legislation? Is it or is it not something which could realistically be achieved consistently with the observance of Convention rights? If it is, then it must be so construed and applied. If, however, it is not, then section 6(2)(b) will apply: the legislation will be incompatible, a declaration of incompatibility may be made, and the public authority will be immune from liability.

145 In short, the question to be asked in deciding whether section 6(2)(b) applies is essentially the same question as is more usually asked under section 3 when deciding whether or not, by a strained construction of apparently incompatible legislation, "it is possible" to read and give effect to it compatibly with Convention rights. Would such a construction depart substantially from a fundamental feature of the legislation? Would it be inconsistent with the underlying thrust of the legislation? Would it go with the grain of the legislation? Would it violate a cardinal principle of the legislation? Would it remove its pith and substance? Would it create an entirely different scheme? The court must not cross the boundary from interpretation into legislation. All these familiar concepts and phrases are to be found in the well known cases on section 3 but their importance has hitherto not perhaps been fully recognised in the context also of section 6(2)(b).

146 It is time to return to section 64(1A) of PACE and in the light of these considerations to ask whether realistically it could be construed for all the world as if, in enacting it, the Government was leaving it to individual police forces—or even to ACPO acting on their joint behalf—to decide upon just what sort of scheme should be implemented for the future retention of biometric data. Is it really suggested that the police could and should then (in 2001) of their own volition have decided that, instead of retaining data indefinitely, they would retain it for only, say, one year or five years, or different periods in different cases and so forth? And if this was not open to them in 2001, how then could it become so merely because of the Grand Chamber's condemnation of the indefinite scheme some years later? As Lord Nicholls of Birkenhead observed in *Ghaidan v Godin-Mendoza* [2004] 2 AC 557, para 33, when indicating the limits of the court's section 3 powers: "There may be several ways of making a provision Convention-compliant, and the choice may involve issues calling for legislative deliberation." It is difficult to think of any case in which that objection to a section 3 construction applies more obviously than here. Lord Steyn reflected the same objection in the same case (para 49): "Interpretation could not provide a substitute scheme." It is surely plain that legislative deliberation was required here.

147 DNA retention can only sensibly operate on a national basis and section 64(1A), properly understood, in my judgment not merely authorised but required precisely the sort of scheme for the indefinite retention of biometric data that the House of Lords came to describe (and, indeed, so enthusiastically to support, in my case unrepentingly) in the *S; Marper* case [2004] 1 WLR 2196. Realistically it was just not possible to construe the section differently, least of all as authorising the police to create for themselves a fundamentally different scheme which would achieve compatibility with the requirements of article 8 as subsequently identified by the Grand Chamber. Of course, some degree of latitude was given to the police as to how precisely the retention scheme was to operate. But this was

257

essentially to decide what narrow categories should be excluded from its scope—cases of the sort described by Lord Steyn at para 36 of the *S; Marper* case (see para 125 above) and, indeed, in the ACPO guidelines: see para 129 above. The discretion could not sensibly be construed as extending to the basic nature of the scheme: whether retention should be indefinite or time-limited.

148 That section 64(1A) was intended to introduce a database for the indefinite retention of DNA samples is surely clear from the very circumstances in which this legislative change was brought about—the deeply disturbing circumstances in which a violent rapist and a brutal murderer had both gone free because of the unsatisfactory existing scheme—see *Attorney General's Reference (No 3 of 1999)* [2001] 2 AC 91 and *In re British Broadcasting Corpn* [2010] 1 AC 145 and, indeed, to my mind clear also from the speeches in the House in the *S and Marper* case to which I have already referred. One of the specific issues before the House in the *S and Marper* case was, it should be noted: "(4) if the retention of fingerprints and DNA profiles and/or samples is an unjustified interference with the appellants' Convention rights, whether it would be possible to give section 64(1A) a Convention-compatible interpretation under section 3 of the 1998 Act" (Lord Steyn's judgment at para 17)—an issue, of course, as Lord Steyn observed at para 57, that in the event fell away. In short, the argument before the House assumed that section 64(1A) called for the indefinite retention of data and that, if this was incompatible with article 8, the appellants then needed to resort to section 3 of HRA for their requests for data removal to succeed.

149 The claimants here submit that, following the Grand Chamber judgment, it was open to the police to adjust their data retention policy to meet the newly recognised requirements of article 8 in just the same way as they were required by this court in *R (L) v Comr of Police of the Metropolis* [2010] 1 AC 410 on article 8 grounds to adjust their previous approach to the disclosure of information for the purposes of enhanced criminal record certificates (ECRCs) pursuant to section 115(7) of the Police Act 1997. In my judgment, however, the two situations are entirely different: in the *L* case all that the court's decision required of the police was that in future they give no less weight to the statutory requirement that in their opinion the information *ought to be* included in the certificate than the requirement that they think it might be relevant (and in borderline cases give the prospective employee an opportunity to say why the information ought not to be disclosed). There was no requirement whatever for fresh policy choices to be made let alone "legislative deliberation" or democratic accountability. Rather the court was well able to decide the limited adjustment that needed to be made.

150 Contrast the position in the present case. The Grand Chamber, in para 134 of its judgment (see para 126 above), can hardly have been expecting the police, rather than the Government, to implement the newly required measures under the supervision of the Committee of Ministers. Correspondingly, the state's reaction to the Grand Chamber's judgment was that it was plainly for Government, not the police, to devise and implement a new and Convention-compliant scheme. It was, indeed, the Home Office rather than the police who decided that children under ten should be removed from the database: see para 127 above. No less significantly, the perceived need for a fully legitimate parliamentary solution to the problem was

258

manifested by the political insistence upon the new scheme being introduced by primary and not merely secondary legislation. If this was not appropriate by secondary legislation, how much less so by revised ACPO guidelines.

151 Even if it is suggested that section 64(1A) does not preclude ACPO from now amending their guidelines to address the Grand Chamber's criticisms in *S v United Kingdom* 48 EHRR 1169, that with respect is not a sufficient answer to the section 6(2)(b) defence. As I have said (para 143 above), the section 6(2)(b) defence necessarily postulates that the public authority *could* act differently. The critical question is whether they could do so consistently with the essential scheme and thrust of the legislation and a good test of that, I would suggest, is to ask whether it can really be said to be their *duty* to do so and to be unlawful and wrong for them *not* to do so. The whole purpose of section 6(2)(b) is to safeguard a public authority from liability (and, indeed, from misplaced criticism) in circumstances where in truth it is acting (as for my part I have no doubt that the police are acting here) perfectly properly.

152 It follows from all this that, in common with Lord Rodger of Earlsferry JSC, with whose judgment on the section 6 issue I respectfully agree, I would hold that it is not unlawful (under domestic law) for the respondent police commissioner to continue to hold the claimants' data on the national DNA database. As to whether this court should now make a declaration of incompatibility in respect of section 64(1A) I hold no strong view. Nowhere is this identified as an issue before us and frankly I find it difficult to see any possible need or use for it in the present circumstances. But if others think it desirable, I would be quite content with that.

153 I would add that, even had I concluded that the police *could* now act compatibly with article 8 under section 64(1A), I should certainly not have thought it "just and appropriate" within the meaning of section 8 of the HRA to require them to change their existing practice pending the introduction of a new legislative data retention scheme. It may be, indeed, that the strength of this reaction to the commissioner's fallback argument under section 8, on true analysis, reinforces the correctness of my primary conclusion on the section 6 issue: quite simply it would be wrong for the police to change their approach to section 64(1A) before Parliament so dictates and this court cannot properly direct them to do so. If anyone is to be criticised for the failure of the existing database to meet the state's obligations under article 8, it is surely the Government, not the police. In my judgment they have a section 6(2)(b) defence to these claims.

Appeals allowed.

JILL SUTHERLAND, Barrister